MOTOROLA SOLUTIONS

DIMETRA™

DIMETRA X Core

Authentication Centre (AuC) User Manual

System Release 9.1.1

MAY 2025

© 2025 Motorola Solutions, Inc. All Rights Reserved.

MN006738A01-B

Intellectual Property and Regulatory Notices

Copyrights

The Motorola Solutions products described in this document may include copyrighted Motorola Solutions computer programs. Laws in the United States and other countries preserve for Motorola Solutions certain exclusive rights for copyrighted computer programs. Accordingly, any copyrighted Motorola Solutions computer programs contained in the Motorola Solutions products described in this document may not be copied or reproduced in any manner without the express written permission of Motorola Solutions.

No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without the prior written permission of Motorola Solutions, Inc.

Trademarks

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

License Rights

The purchase of Motorola Solutions products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications of Motorola Solutions, except for the normal non-exclusive, royalty-free license to use that arises by operation of law in the sale of a product.

Open Source Content

This product may contain Open Source software used under license. Refer to the product installation media for full Open Source Legal Notices and Attribution content.

European Union (EU) and United Kingdom (UK) Waste of Electrical and Electronic Equipment (WEEE) Directive

The European Union's WEEE directive and the UK's WEEE regulation require that products sold into EU countries and the UK must have the crossed-out wheelie bin label on the product (or the package in some cases). As defined by the WEEE directive, this crossed-out wheelie bin label means that customers and end-users in EU and UK countries should not dispose of electronic and electrical equipment or accessories in household waste.

Customers or end-users in EU and UK countries should contact their local equipment supplier representative or service centre for information about the waste collection system in their country.

Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a specific system, or may be dependent upon the characteristics of a specific mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola Solutions contact for further information.

© 2025 Motorola Solutions, Inc. All Rights Reserved

CMM Labeling and Disclosure Table

The People's Republic of China requires that our products comply with China Management Methods (CMM) environmental regulations. (China Management Methods refers to the Regulation Management Methods for Controlling Pollution by Electronic Information Products.) Two items are used to demonstrate compliance; the Label and the Disclosure Table.

The label is placed in a customer visible position on the product. The first of the following examples means that the product contains no hazardous substances; the second means that the product contains hazardous substances, and has an Environmental Friendly Use Period (EFUP) of fifty years.

The Environmental Friendly Use Period (EFUP) is the period (in years) during which the Toxic and Hazardous Substances contained in the Electronic Information Product (EIP) will not leak or mutate causing environmental pollution, or bodily injury from the use of the EIP.

The Disclosure Table, printed in simplified Chinese, is included with each customer order. An example of a Disclosure Table (in Chinese) follows:

Disclosure table

部件名称	有毒有害物质或元素					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr^{6+})	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
金属部件	×	○	×	×	○	○
电路模块	×	○	×	×	○	○
电缆及电缆组件	×	○	×	×	○	○
塑料和聚合物部件	○	○	○	○	○	×

本表格依据 SJ/T 11364 的规定编制。
O：表示该有毒有害物质在该部件所有均质材料中的含量均在 GB/T 26572 标准规定的限量要求以下。
X：表示该有毒有害物质至少在该部件的某一均质材料中的含量超出 GB/T 26572 标准规定的限量要求。

Service Information

Technical & Repair Support (for Contracted Customers Only)

If you would like to contact the Motorola Solutions Customer Care team, use the appropriate contact details below. Please be prepared to provide your contract number, product serial numbers, and detailed issue description for a faster response and a resolution. If the support request is Technical Support related, the request will be handled by the Technical Support Operations (TSO) team. This team of highly skilled professionals provides Technical Support to help resolve technical issues and quickly restore networks and systems. If you are unsure whether your current service agreement entitles you to benefit from this service, or if you would like more information about the Technical or Repair Support Services, contact your local customer support or account manager for further information.

Contact Details

Technical Requests: techsupport.emea@motorolasolutions.com

Repair Support: repair.emea@motorolasolutions.com

Contact Us: https://www.motorolasolutions.com/en_xu/support.html

Parts Identification and Ordering

If you need help in identifying non-referenced spare parts, direct a request to the Customer Care Organization of a local area Motorola Solutions representative. Orders for replacement parts, kits, and assemblies should be placed directly at the local distribution organization of Motorola Solutions or through the Extranet site Motorola Online at https://emeaonline.motorolasolutions.com.

Document History

Version	Description	Date
MN006738A01-A	Initial version.	June 2020
MN006738A01-B	Updated: ● Installing the External Modem Driver for KVL to AuC/PrC Communication on page 74 ● Loading Keys with Serial Connection on page 150	May 2025

Contents

Intellectual Property and Regulatory Notices....2
CMM Labeling and Disclosure Table....3
Service Information....4
Document History....5
List of Figures....14
List of Tables....16
List of Processes....19
List of Procedures....20
About Authentication Centre (AuC) User Manual....23
What Is Covered in This Manual?....23
Related Information....23
Icon Conventions....25
Style Conventions....26
Chapter 1: AuC Description....27
1.1 Introduction to Authentication Centre....27
1.2 AuC, PrC and AIE Introduction....27
1.3 Enhanced Authentication Centre....27
1.4 Authentication Centre....28
1.4.1 What is the Authentication Centre?....28
1.4.2 Authentication Centre Client....28
1.4.2.1 Automatic Detection of Network Problems....28
1.4.3 Authentication Centre Server....28
1.4.4 Authentication Centre Database....29
1.5 Implementing Your Security Policy....29
1.5.1 Planning Your Steps....29
1.5.2 Technical Implementation Steps....30
Chapter 2: AuC Client Interface Reference....31
2.1 Main Window Structure....31
2.1.1 Authentication Centre Main Window....31
2.1.2 The Work Pane....32
2.1.3 The Events Pane....32
2.1.4 Status Bar....32
2.1.5 The Menu Bar....33
2.2 Main Window Elements....33
2.2.1 AuC Comm Key (Communication Key)....34

2.2.2 AuC Connectivity....35
2.2.3 AuC Net....36
2.2.4 Audit Search and Purge Form....37
2.2.4.1 Audit Trail Information Display....38
2.2.5 CMGs Tree View Display....38
2.2.6 CMG Information....39
2.2.7 DDK (DIMETRA Distribution Key)....40
2.2.8 BTS Site Information....40
2.2.9 Events Information....41
2.2.10 AuC Connectivity Information....41
2.2.11 K-REF Pairs....43
2.2.12 Transfer KRefs....44
2.2.13 Key Database Selection....45
2.2.14 Key Schedule Information....45
2.2.15 Key Schedules Selection....46
2.2.16 Key Status Tree View....46
2.2.17 KVL Information....47
2.2.18 KVL Status List View....48
2.2.19 Mapping Types Display....48
2.2.20 Mobile Stations List....48
2.2.21 Operational Group Information....50
2.2.22 OTAR Progress Information....50
2.2.23 Mobile Station Search Form....51
2.2.24 Mobiles OTAR Keys Reporting....52
2.2.25 Raw Keys Management....53
2.2.26 SCK-Trunked Mode Operation Information....53
2.2.27 Security Group Selection Tree View....54
2.2.28 UCS Information....54
2.2.29 User Account Selection Tree View....55
2.2.30 User Information....55
2.2.31 Zone Information....57
2.3 Secondary Window....57
2.3.1 Add User Dialog Box....58
2.3.2 AuC Connection....59
2.3.3 AuC Backup Dialog Box....60
2.3.4 Change Password Dialog Box....60
2.3.5 Encryption Devices Dialog Box....61
2.3.6 Key Update Lock Details Information Box....62
2.3.7 Key Update Lock Dialog Box....62
2.3.8 Key Report Contents Dialog Box....63

2.3.9 KVL UKEK Assignment Dialog Box.... 63
2.3.10 Login Dialog Box.... 64
2.3.11 Miscellaneous Settings.... 64
2.3.12 Server Settings.... 64
2.3.13 Port Settings.... 65
2.3.14 Purge Audit Trail Dialog Box.... 66
2.3.15 SAI Cache Settings.... 66
2.3.16 SCK-TMO Modify Dialog Box.... 67
2.3.17 User Settings.... 67
2.3.18 Thresholds Settings.... 68
2.3.19 AuC Database Standby Manager Icon Descriptions.... 69
2.3.20 AuC Database Standby Manager Window Description.... 69
2.4 Main Menu Items.... 70
Chapter 3: AuC Installation and Configuration.... 72
3.1 AuC Server Application Installation.... 72
3.2 User Account Control.... 72
3.3 GUI Applications Access Permissions.... 72
3.4 Installing the Enhanced Authentication Centre Client Application.... 72
3.5 Configuring AuC after Installation.... 73
3.6 Installing the External Modem Driver for KVL to AuC/PrC Communication.... 74
3.7 Configuring KVL Port Settings.... 75
Chapter 4: AuC Basic Operation.... 77
4.1 First Steps.... 77
4.1.1 Starting the Authentication Centre Client Application.... 77
4.1.2 Changing View.... 77
4.1.3 Changing a User Account Password.... 78
4.1.4 Verifying Authentication Centre Status.... 78
4.1.5 Displaying Key and Entity Information.... 78
4.1.6 Logging off from the Authentication Centre Client Application.... 78
4.2 Getting Help.... 79
4.2.1 Using Context Sensitive Help.... 79
4.2.2 Using Full Text Search.... 79
4.3 Changing Authentication Centre Operating State.... 79
4.4 Viewing Enhanced Authentication Centre Version Information.... 80
4.5 Generating Key Reports.... 80
4.6 Users.... 80
4.6.1 Creating an Enhanced AuC User Account.... 81
4.6.2 Modifying an Existing User Account.... 81
4.6.3 Deleting an AuC User Account.... 81
4.7 Events.... 81

4.7.1 Sorting Authentication Centre Events....82
4.7.2 Removing Authentication Centre Events....82
4.8 Audits....83
4.8.1 Viewing Event Audits....83
4.8.2 Removing Audits Data from the Database....83
Chapter 5: Authentication and Air Interface Encryption Key Management....85
5.1 Entity Status and Key Information....85
5.1.1 Radio Key Information....85
5.1.2 Viewing Radio Key Information....86
5.1.3 Generating Radio Report....87
5.1.4 Generating Mobiles OTAR Keys Report....87
5.1.5 Viewing and Deleting Unmatched K-REF Pairs....88
5.1.6 Generating an Unmatched K-Ref Pairs Report....90
5.1.7 Zone Status and Key Information....91
5.1.8 Viewing Zone Status and Key Information....91
5.1.9 Site Status and Key Information....91
5.1.10 Viewing Site Status and Key Information....92
5.1.11 Viewing UCS Status....92
5.1.12 ZDS Status....93
5.1.13 Viewing KVL Key Information and Status....93
5.2 Entering and Modifying Keys....94
5.2.1 Entering K-REF Pairs into the Authentication Centre....94
5.2.2 Transfering K-REF Pairs into the Authentication Centre....95
5.2.3 Importing a K-REF Pair File into the Authentication Centre....96
5.2.4 Importing an SCK-TMO Key File into the Authentication Centre....97
5.2.5 Modifying an SCK-TMO Key in the Authentication Centre....98
5.2.6 Setting the Next Active SCK-TMO Key....99
5.2.7 Changing Trunked Mode Operation....100
5.2.8 Changing Key Usage Mode....101
5.2.9 Entering the AuC Communications Key....102
5.2.10 Entering a DIMETRA Distribution Key....103
5.2.11 Generating Raw Keys Automatically....103
5.2.12 Retrieving Raw Keys from the Imported File....104
5.2.13 Importing Raw Keys from a File....105
5.2.14 Entering a UKEK Key for a KVL Device....105
5.3 Key Distribution....106
5.3.1 Logging On to the Server....106
5.3.1.1 Messages Appearing when Establishing a Secure Session....107
5.3.2 Logging On to iGAS Through a KVM Switch....108
5.3.3 Attaching Device to Serial Port....109

5.3.4 Provisioning Zone or Site Entity with an Infrastructure Key....109
5.3.4.1 Loading an Infrastructure Key (Ki) to a Site Entity....110
5.3.5 Reprovisioning Zone Entity with an Existing Infrastructure Key....111
5.3.5.1 Refreshing a Ki for Selected Zone Entity....112
5.3.6 Reprovisioning Zone or Site Entity with a New Infrastructure Key....112
5.3.6.1 Updating a Ki Key for a Zone or Site Entity....113
5.3.7 Clearing an Infrastructure Key from a Zone or BTS Site Entity....113
5.3.8 Scheduling Key Updates....113
5.3.9 Performing Immediate Key Updates....114
5.3.10 Assigning New Authentication Material for a Radio....115
5.3.11 Reversing USB Order....116
5.4 Clearing a Radio....117
5.5 Enabling and Disabling Key Updates....117
5.5.1 Enabling/Disabling Key Updates for a Radio....118
5.5.2 Enabling/Disabling Key Updates for a Zone....119
5.5.3 Enabling/Disabling Key Updates for a Site....119
5.5.4 Resetting a Site....119
5.5.5 Enabling/Disabling Key Updates By Key Type....120
5.5.6 Enabling/Disabling KVL Access to the Authentication Centre....120
Chapter 6: Crypto Management Group Configuration....122
6.1 Importing Mapping Files....122
6.2 Exporting CMG Mappings....122
6.3 Enabling CMGs....123
6.4 Assigning GCKNs and KAGNs....123
6.5 Creating CMGs....123
6.6 Removing CMGs....124
6.7 Creating ISSI Ranges....124
6.8 Removing ISSI Ranges....124
6.9 Creating Operational Groups....124
6.10 Removing Operational Groups....125
6.11 Creating GSSI Ranges....125
6.12 Removing GSSI Ranges....125
6.13 Enabling CMG Configuration....126
6.14 Editing Enabled CMG Configuration....126
6.15 Disabling CMG Configuration....126
6.16 OTAR Configuration....127
6.17 Disabling OTAR....127
Chapter 7: Nationwide AuC Configuration....128
7.1 Viewing AuC Connection Information and Status....128
7.2 Nationwide AuC System Configuration....130

7.2.1 Configuring Nationwide Master AuC....131
7.2.2 Configuring Nationwide Slave AuC....132
7.2.3 Rejected Key Update Event Log Messages....133
7.3 Key Updates in the Nationwide System....134
7.4 Slave AuCs Reconfiguration in the Nationwide System....134
7.4.1 Adding a New Slave AuC to the Nationwide System....135
7.4.2 Changing Expected Slave AuC....135
7.4.3 Removing Expected Slave AuC....135
7.4.4 Removing Slave AuC from the Nationwide System....136
7.5 Returning to the Single Cluster Mode....136
7.6 Nationwide AuC System Reconfiguration....136
7.6.1 Connecting Slave AuC to Another Master....137
7.6.2 Changing Master in the Nationwide System....137
Chapter 8: AuC System Settings....139
8.1 Configuring Authentication Centre Operation Settings....139
8.1.1 Configuring KVL Port Settings....139
8.1.2 Configuring Miscellaneous Settings....140
8.1.3 Configuring Server Settings....140
8.1.4 Configuring User Settings....141
8.1.5 Configuring SAI Cache Settings....141
8.1.6 Configuring Thresholds Settings....141
Chapter 9: Encryption Device Configuration....143
9.1 Viewing Encryption Device Status....143
9.2 Encryption Device Information....143
9.3 CryptR2 Configuration for Standby AuC....144
9.4 Upgrading the CryptR2 Software Through TFTP....144
9.4.1 TFTP Upgrade Failure – Troubleshooting....146
9.5 Configuring CryptR2....146
9.6 Setting Up CryptR2....146
9.7 Entering User and Admin Password....147
9.8 Entering AES Master Key....148
9.9 Loading Master Keys into an Encryption Device....148
9.10 Loading Keys with Serial Connection....150
9.11 Verifying DVI-XL Master Keys....152
9.12 Changing DVI-XL Master Keys....153
9.13 Requesting Logs from an Encryption Device....154
Chapter 10: System Management....155
10.1 Windows Local Groups....155
10.2 Config Assistant Access....155
10.3 AuC Standby Feature....155

10.3.1 AuC Roles....155
10.3.2 Database Standby Manager....155
10.3.2.1 GUI Client....156
10.3.2.2 Checking Standby Status....156
10.3.3 AuC Roles Management....156
10.3.3.1 Checking AuC Current Role....156
10.3.3.2 Switching Roles of AuC Servers....157
10.3.3.3 Managing AuC Roles after Failure of Active AuC....158
10.3.3.4 Managing AuC Roles after Failure of Standby AuC....158
10.3.3.5 Changing the Role of the Standby AuC to Active AuC....158
Chapter 11: AuC Maintenance....159
11.1 Backing up the Database....159
Chapter 12: Troubleshooting the AuC....160
12.1 Basic Troubleshooting....160
12.1.1 Common AuC Start-up Error Messages....160
12.1.2 AuC Troubleshooting Scenarios....161
12.1.3 Scenarios when Performing Key Updates....164
12.1.3.1 Scenario 1 Key Update Stuck (Local Cluster)....164
12.1.3.2 Scenario 2 Authentication Material Update Stuck (Local Cluster)....165
12.1.3.3 Scenario 3 Nationwide Update Stuck (Nationwide)....165
12.1.4 Restarting AuC....166
12.1.5 Recovering CryptR2 from Tampered State....166
12.1.6 Key Distribution Failure....167
12.1.6.1 Normal Operation....167
12.1.6.2 Follow Up Action....167
12.2 Known Issues....167
12.2.1 Some Connections Between AuC and KVL Stops Because of AuC Inactivity....167
12.2.1.1 Resolution/Workaround....168
12.2.2 Database Failure....168
12.2.2.1 Resolution/Workaround....168
12.3 Handling Compromised Units....168
12.3.1 Temporary Disabling/Enabling a Radio....168
12.3.1.1 Opening the Radio Command Window in the RCM....169
12.3.1.2 Temporarily Disabling a Radio from Operating on the System....169
12.3.2 Permanently Disabling a Radio....170
12.4 FAQ....171
12.4.1 Key Management....171
12.4.1.1 How are Keys Provisioned in the DIMETRA System?....172
12.4.1.2 How are Keys Stored in the DIMETRA System?....172
12.4.1.3 How are Keys Updated in the DIMETRA System?....172

12.4.1.4 What Do I Do if a Key is not Current?....172
12.4.1.5 When Should I Perform an Audit Trail Search?....173
12.4.1.6 Key Update Stages....173
12.4.2 Radios....173
12.4.2.1 What Do I Do if a K-REF Pair is Unmatched?....174
12.4.2.2 When Should I Delete Unmatched K-REF Pairs?....174
12.4.3 General Problems....174
12.4.3.1 How to Trigger Full Synchronization with UCS....174
12.4.3.2 Triggering Full Synchronization with ZDS....175
12.4.3.3 What Happens if a Key Update Fails?....175
12.4.3.4 What Do I Do if the Database Fails?....175
12.4.3.5 What Do I Do if an Encryption Device Fails?....175
12.4.3.6 What to Do if an Error Message Appears when Starting the Client?....175
12.4.4 Implementing and Enabling GCK/OTAR....176
12.4.4.1 Good Practices....178
12.4.5 Security Class 3 Configuration Changes....179
Chapter 13: Config Assistant....180

List of Figures

Figure 1: The EAuC Main Window....31
Figure 2: The Work Pane – Encrypted AuC Example....32
Figure 3: The Events Pane....32
Figure 4: Status Bar - Example....33
Figure 5: AuC Comm Key (Communication Key) Display....34
Figure 6: AuC Connectivity Display....35
Figure 7: AuC Net Pane Example....36
Figure 8: Audit Search Purge Form....37
Figure 9: Events Pane....41
Figure 10: AuC Connectivity Information Display....42
Figure 11: Key Schedule Information Display - Example....45
Figure 12: Mobile Stations Search Form Pane....51
Figure 13: Security Group Selection Tree View....54
Figure 14: User Account Selection Display....55
Figure 15: User Information Display....55
Figure 16: Add User Dialog Box....58
Figure 17: The Mobile Station Search Form - Example....86
Figure 18: Mobile Station Search Form....87
Figure 19: The Keys Tabbed Pane Example....89
Figure 20: Keys Pane....90
Figure 21: K-Ref Pairs Pane....90
Figure 22: KVLs Pane Example....93
Figure 23: Keys Pane....94
Figure 24: K-REF Pairs Pane....95
Figure 25: Keys Pane....96
Figure 26: Keys Pane Example....96
Figure 27: Keys Pane....97
Figure 28: Key Pane....98
Figure 29: SCK-TMO (Static Cipher Key - Trunked Mode Operation) Pane....98
Figure 30: Keys Pane....99
Figure 31: SCK-Trunked Mode Operation Display - Example....100
Figure 32: Keys Tabbed Pane....101
Figure 33: SCK-Trunked Mode Operation Display - Example....102
Figure 34: Keys Pane....102
Figure 35: Keys Pane....103
Figure 36: Keys Pane....104

Figure 37: Keys Pane..... 104
Figure 38: KVLs Tabbed Pane Example..... 105
Figure 39: Mobile Station Search Form - Example..... 116
Figure 40: Full Synchronization with UCS - Example..... 117
Figure 41: Mobiles List - Example..... 117
Figure 42: Mobile Station Search Form - Example..... 118
Figure 43: AuC Net Pane Example..... 129
Figure 44: AuC Connectivity Pane Example..... 130
Figure 45: AuC Net Pane Example..... 132
Figure 46: AuC Net Pane Example..... 133
Figure 47: CryptR2 Connection Diagram..... 145
Figure 48: Encryption Device Dialog Box..... 148
Figure 49: Encryption Device Dialog Box..... 149
Figure 50: Database Standby Manager System Tray Icon..... 156
Figure 51: AuC Backup Dialog Box..... 159
Figure 52: The Status Bar During Database Backup..... 159

List of Tables

Table 1: Security Planning Questions....29
Table 2: Enhanced Authentication Centre (EAuC) States of Operation....33
Table 3: Enhanced AuC Connection Status Icons....33
Table 4: Fields in the AuC Comm Key (Communication Key) Display....34
Table 5: Buttons in the AuC Comm Key (Communication Key) Display....34
Table 6: Fields in the AuC Connectivity Information Display....35
Table 7: AuC Server Status Information and Icons....37
Table 8: Fields in the Audit Search Purge Form display....37
Table 9: Buttons in the Audit Search Purge Form display....38
Table 10: Fields in the Audit Trail Information display....38
Table 11: Operational Group Icons....39
Table 12: Buttons in the CMG Tree View Display....39
Table 13: Fields in the CMG Information Display....39
Table 14: Buttons in the CMG Information Display....39
Table 15: Fields in the DDK Information display....40
Table 16: Buttons in the DDK Information display....40
Table 17: Fields in the BTS Site Information display....40
Table 18: Buttons in the BTS Site Information display....41
Table 19: Fields in the Events Information Display....41
Table 20: Buttons in the Events Information Display....41
Table 21: Fields in the AuC Connectivity Information Display....42
Table 22: Fields in the K-REF Pairs Information Display....43
Table 23: Buttons in the K-REF Pairs Information Display....43
Table 24: Fields in the Transfer KRefs Window....44
Table 25: Fields in the Key Database Selection Display....45
Table 26: Fields in the Key Schedule Information Display....46
Table 27: Buttons in the Key Schedule Information Display....46
Table 28: Fields in the Key Update Selection Display....46
Table 29: Key Status Icons (Zones and sites)....47
Table 30: Fields in the KVL Information Display....47
Table 31: Buttons in the KVL Information Display....47
Table 32: Key Status Icons (KVLs)....48
Table 33: Buttons in the Mapping Types Display....48
Table 34: Fields in the Mobile Stations List Pane....48
Table 35: Buttons in the Mobile Stations List Pane....49
Table 36: Fields in the Operational Group Information Display....50

Table 37: Buttons in the Operational Group Information Display..... 50
Table 38: Fields in the OTAR Progress Information Display..... 50
Table 39: Buttons in the OTAR Progress Information Display..... 50
Table 40: Fields in the Mobile Stations Search Form Pane.....51
Table 41: Buttons in the Mobile Stations Search Form Pane..... 51
Table 42: Fields in the Mobiles OTAR Key Report Display..... 52
Table 43: Buttons in the Mobiles OTAR Keys Report Display..... 52
Table 44: Fields in the Raw Keys Management Display..... 53
Table 45: Buttons in the Raw Keys Management Display..... 53
Table 46: Fields in the SCK-Trunked Mode Operation Information Display..... 53
Table 47: Buttons in the SCK-Trunked Mode Operation Information Display..... 53
Table 48: Fields in the UCS Information Display.....54
Table 49: Buttons in the UCS Information Display.....54
Table 50: Fields in the User Information Display..... 56
Table 51: Access Permissions for AuC Users..... 56
Table 52: Buttons in the User Information Display..... 56
Table 53: Fields in the Zone Information Display..... 57
Table 54: Buttons in the Zone Information Display..... 57
Table 55: Fields in the Add User Dialog Box..... 58
Table 56: Access Permissions for AuC Users..... 58
Table 57: Buttons in the Add User Dialog Box..... 59
Table 58: Fields in the AuC Connection Display..... 59
Table 59: Buttons in the AuC Connection Display..... 59
Table 60: Fields in the AuC Backup Dialog Box..... 60
Table 61: Buttons in the AuC Database Dialog Box.....60
Table 62: Fields in the Change Password Dialog Box..... 60
Table 63: Buttons in the Change Password Dialog Box..... 61
Table 64: Fields in the Encryption Devices Dialog Box.....61
Table 65: Buttons in the Encryption Devices Dialog Box.....62
Table 66: Field in the Key Update Lock Details Information Box..... 62
Table 67: Buttons in the Key Update Lock Details Information Box..... 62
Table 68: Field in the Key Update Lock Dialog Box.....62
Table 69: Buttons in the Key Update Lock Dialog Box.....62
Table 70: Fields in the Key Report Contents Window.....63
Table 71: Fields in the KVL UKEK Assignment Dialog Box..... 63
Table 72: Buttons in the KVL UKEK Assignment Dialog Box..... 63
Table 73: Fields in the Login Dialog Box..... 64
Table 74: Buttons in the Login Dialog Box..... 64
Table 75: Fields Shown in the Preferences Dialog Box when the Miscellaneous Entity is Selected.....64

Table 76: Buttons Shown in the Preferences Dialog Box when the Miscellaneous Entity is Selected.....64
Table 77: Fields Shown in the Preferences Dialog Box when Server Settings are Selected.....64
Table 78: Buttons Shown in the Preferences Dialog Box when Server Settings are Selected.....65
Table 79: Fields Shown in the Preferences Dialog Box when the Port Settings Entity is Selected.....65
Table 80: Buttons Shown in the Preferences Dialog Box when the Port Settings Entity is Selected.....65
Table 81: Fields in the Purge Audit Trail Dialog Box.....66
Table 82: Buttons in the Purge Audit Trail Dialog Box.....66
Table 83: Fields Shown in the Preferences Dialog Box when the SAI Cache Entity is Selected.....66
Table 84: Buttons Shown in the Preferences Dialog Box when the SAI Cache Entity is Selected.....66
Table 85: Fields in the SCK-TMO Modify Dialog Box.....67
Table 86: Buttons in the SCK-TMO Modify Dialog Box.....67
Table 87: Fields Shown in the Preferences Dialog Box when the User Settings Entity is Selected.....67
Table 88: Buttons Shown in the Preferences Dialog Box when the User Settings Entity is Selected.....68
Table 89: Fields Shown in the Preferences Dialog Box when the Thresholds Entity is Selected.....68
Table 90: Buttons Shown in the Preferences Dialog Box when the Thresholds Entity is Selected.....68
Table 91: AuC Server Standby Status Information Icon.....69
Table 92: Fields in the Database Standby Manager window.....69
Table 93: Buttons in the Database Standby Manager window.....70
Table 94: Main Menu Items.....70
Table 95: Using Context Sensitive Help.....79
Table 96: Messages Appearing when Establishing a Secure Session.....107
Table 97: Rejected Key Update Event Log Messages.....133
Table 98: Common Client Startup Error Messages and Descriptions.....160
Table 99: Troubleshooting the AuC.....161
Table 100: Scenario 1.....164
Table 101: Scenario 2.....165
Table 102: Scenario 3.....165
Table 103: Key Update Stages.....173
Table 104: Common Error Messages.....175
Table 105: Config Assistant Commands.....180
Table 106: Optional Arguments for CA Commands.....182

List of Processes

Provisioning Zone or Site Entity with an Infrastructure Key 109
Reprovisioning Zone Entity with an Existing Infrastructure Key 111
Reprovisioning Zone or Site Entity with a New Infrastructure Key 112
Nationwide AuC System Configuration 130
Key Updates in the Nationwide System 134
TFTP Upgrade Failure – Troubleshooting 146
Configuring CryptR2 146
Implementing and Enabling GCK/OTAR 176

List of Procedures

Installing the Enhanced Authentication Centre Client Application 72
Configuring AuC after Installation 73
Installing the External Modem Driver for KVL to AuC/PrC Communication 74
Configuring KVL Port Settings 75
Starting the Authentication Centre Client Application 77
Changing a User Account Password 78
Displaying Key and Entity Information 78
Logging off from the Authentication Centre Client Application 78
Changing Authentication Centre Operating State 79
Generating Key Reports 80
Creating an Enhanced AuC User Account 81
Modifying an Existing User Account 81
Deleting an AuC User Account 81
Sorting Authentication Centre Events 82
Removing Authentication Centre Events 82
Viewing Event Audits 83
Removing Audits Data from the Database 83
Viewing Radio Key Information 86
Generating Radio Report 87
Generating Mobiles OTAR Keys Report 87
Viewing and Deleting Unmatched K-REF Pairs 88
Generating an Unmatched K-Ref Pairs Report 90
Viewing Zone Status and Key Information 91
Viewing Site Status and Key Information 92
Viewing UCS Status 92
Viewing KVL Key Information and Status 93
Entering K-REF Pairs into the Authentication Centre 94
Transfering K-REF Pairs into the Authentication Centre 95
Importing a K-REF Pair File into the Authentication Centre 96
Importing an SCK-TMO Key File into the Authentication Centre 97
Modifying an SCK-TMO Key in the Authentication Centre 98
Setting the Next Active SCK-TMO Key 99
Changing Trunked Mode Operation 100
Changing Key Usage Mode 101
Entering the AuC Communications Key 102
Entering a DIMETRA Distribution Key 103

Generating Raw Keys Automatically 103
Retrieving Raw Keys from the Imported File 104
Importing Raw Keys from a File 105
Entering a UKEK Key for a KVL Device 105
Logging On to the Server 106
Logging On to iGAS Through a KVM Switch 108
Attaching Device to Serial Port 109
Loading an Infrastructure Key (Ki) to a Site Entity 110
Refreshing a Ki for Selected Zone Entity 112
Updating a Ki Key for a Zone or Site Entity 113
Scheduling Key Updates 113
Performing Immediate Key Updates 114
Assigning New Authentication Material for a Radio 115
Reversing USB Order 116
Clearing a Radio 117
Enabling/Disabling Key Updates for a Radio 118
Enabling/Disabling Key Updates for a Zone 119
Enabling/Disabling Key Updates for a Site 119
Resetting a Site 119
Enabling/Disabling Key Updates By Key Type 120
Enabling/Disabling KVL Access to the Authentication Centre 120
Importing Mapping Files 122
Exporting CMG Mappings 122
Enabling CMGs 123
Assigning GCKNs and KAGNs 123
Creating CMGs 123
Removing CMGs 124
Creating ISSI Ranges 124
Removing ISSI Ranges 124
Creating Operational Groups 124
Removing Operational Groups 125
Creating GSSI Ranges 125
Removing GSSI Ranges 125
Enabling CMG Configuration 126
Editing Enabled CMG Configuration 126
Disabling CMG Configuration 126
OTAR Configuration 127
Disabling OTAR 127
Viewing AuC Connection Information and Status 128

Configuring Nationwide Master AuC 131
Configuring Nationwide Slave AuC 132
Adding a New Slave AuC to the Nationwide System 135
Changing Expected Slave AuC 135
Removing Expected Slave AuC 135
Removing Slave AuC from the Nationwide System 136
Returning to the Single Cluster Mode 136
Connecting Slave AuC to Another Master 137
Changing Master in the Nationwide System 137
Configuring KVL Port Settings 139
Configuring Miscellaneous Settings 140
Configuring Server Settings 140
Configuring User Settings 141
Configuring SAI Cache Settings 141
Configuring Thresholds Settings 141
Viewing Encryption Device Status 143
CryptR2 Configuration for Standby AuC 144
Upgrading the CryptR2 Software Through TFTP 144
Setting Up CryptR2 146
Entering User and Admin Password 147
Entering AES Master Key 148
Loading Master Keys into an Encryption Device 148
Loading Keys with Serial Connection 150
Verifying DVI-XL Master Keys 152
Changing DVI-XL Master Keys 153
Requesting Logs from an Encryption Device 154
Checking AuC Current Role 156
Switching Roles of AuC Servers 157
Changing the Role of the Standby AuC to Active AuC 158
Backing up the Database 159
Restarting AuC 166
Recovering CryptR2 from Tampered State 166
Opening the Radio Command Window in the RCM 169
Temporarily Disabling a Radio from Operating on the System 169
Permanently Disabling a Radio 170
How to Trigger Full Synchronization with UCS 174
Triggering Full Synchronization with ZDS 175
Security Class 3 Configuration Changes 179

About Authentication Centre (AuC) User Manual

This manual describes the Authentication Centre (AuC) application. It contains operation and troubleshooting procedures necessary to successfully manage authentication and air interface encryption features.

What Is Covered in This Manual?

This manual covers the management of the authentication and air interface encryption features in the DIMETRA system. This manual includes the following topics:

- Processes and procedures for managing operation of the authentication and air interface encryption feature
- Processes and procedures for managing encryption keys in the system infrastructure
- Description of the different aspects of secure encryption key management

This manual does not provide specific procedures for distributing keys using the Motorola Provisioning Centre (PrC) or Key Variable Loader (KVL) tools. Where appropriate, you are referred to the relevant manuals for that information.

The purpose of this manual is to provide you with the information that you need to use the Authentication Centre (AuC) application.

The material covered in this manual is presented in the following chapters:

- AuC Description on page 27
- AuC Client Interface Reference on page 31
- AuC Installation and Configuration on page 72
- AuC Basic Operation on page 77
- Authentication and Air Interface Encryption Key Management on page 85
- Crypto Management Group Configuration on page 122
- Nationwide AuC Configuration on page 128
- AuC System Settings on page 139
- Encryption Device Configuration on page 143
- System Management on page 155
- AuC Maintenance on page 159
- Troubleshooting the AuC on page 160
- Config Assistant on page 180

Related Information

Document Title	Description
Glossary	The glossary provides definitions of terms, abbreviations, and acronyms used in the DIMETRA system documentation.

Document Title	Description
Documentation Overview	This document provides a list of all documents delivered with your DIMETRA system.
System Overview	This manual explains basic radio system concepts, call processing basics, and an introduction to the various components and processes associated with the DIMETRA system. The manual provides the background needed to comprehend DIMETRA system theory of operation. It also provides functional descriptions of equipment and subsystems, and describes the role of the numerous network management software applications used in the system.
HP ProLiant Gen9 Server Platform Restoration	This manual describes how to restore a Gen9 server platform in case of a failure.
Provisioning Centre (PrC) User Manual	This manual describes how to use the Provisioning Centre (PrC) application. The main functions of the Provisioning Centre are: • Providing secure (encrypted) storage of subscriber keys • Providing secure upload and download facilities for subscriber keys and key data • Displaying up-to-date information about the key status of the radios • Exporting K-Ref data to permanent storage media • Generating audit trail and radio information.
DIMETRA KVL 4000 AIE and Authentication User Guide	This manual provides instructions for using the KVL 4000 Key Variable Loader to perform Air Interface Encryption and Authentication operations in Motorola DIMETRA systems.
DIMETRA KVL 4000 Authentication User Guide	This manual provides instructions for using the KVL 4000 Key Variable Loader to perform Authentication operations in Motorola DIMETRA systems.
CryptR Instruction Manual	This manual covers hardware installation, main end-user operations and a proper maintenance of a range of devices based on the CryptR hardware platform.

Icon Conventions

The documentation set is designed to give the reader more visual clues. The following graphic icons are used throughout the documentation set.

DANGER: The signal word DANGER with the associated safety icon implies information that, if disregarded, will result in death or serious injury.

WARNING: The signal word WARNING with the associated safety icon implies information that, if disregarded, could result in death or serious injury, or serious product damage.

CAUTION: The signal word CAUTION with the associated safety icon implies information that, if disregarded, may result in minor or moderate injury, or serious product damage.

CAUTION: The signal word CAUTION may be used without the safety icon to state potential damage or injury that is not related to the product.

IMPORTANT: IMPORTANT statements contain information that is crucial to the discussion at hand, but is not CAUTION or WARNING. There is no warning level associated with the IMPORTANT statement.

NOTE: NOTICE contains information more important than the surrounding text, such as exceptions or preconditions. They also refer the reader elsewhere for additional information, remind the reader how to complete an action (when it is not part of the current procedure, for instance), or tell the reader where something is on the screen. There is no warning level associated with a notice.

Style Conventions

The following style conventions are used:

Convention	Description
Bold	This typeface is used for names of, for instance, windows, buttons, and labels when these names appear on the screen (example: the **Alarms Browser** window). When it is clear that we are referring to, for instance, a button, the name is used alone (example: Click **OK**).
`Monospacing font`	This typeface is used for words to be typed in exactly as they are shown in the text (example: In the **Username** field, enter: `Admin`).
	This typeface is used for messages, prompts, and other text displayed on the computer screen (example: `A new trap destination has been added`).
`<Monospacing font in bold Italic>`	This typeface is used with angle brackets as placeholders for a specific member of the group that the words represent (example: *`<router number>`*). **NOTE:** In sequences to be typed in, the angle brackets are omitted to avoid confusion whether to include the angle brackets in the text to be typed.
CAPITAL LETTERS	This typeface is used for keyboard keys (example: Press Y and press ENTER).
Italic	This typeface is used for citations. A citation usually is the name of a document or a phrase from another document (example: *DIMETRA System Overview*).
→	An → (arrow pointing right) is used for indicating the menu or tab structure in instructions on how to select a certain menu item (example: **File** → **Save**) or a certain sub-tab.

Chapter 1

AuC Description

1.1 Introduction to Authentication Centre

The Authentication Centre (AuC) is a client/server software application that handles encryption key management duties for the Motorola DIMETRA two-way radio system. The AuC handles distribution, storage, and update of encryption keys used by the DIMETRA systems Authentication and Air Interface Encryption feature.

The AuC provides the following features:

- Up-to-date display of key currency status for appropriate DIMETRA radio system infrastructure devices.
- Central location for secure storage of both infrastructure and subscriber device keys. Keys can be imported via file, typed in using keyboard, or generated by the AuCs encryption device (CryptR2).
- Scheduled or on-demand key updates of infrastructure devices using secure distribution methods.
- Unique authentication key material that enables the system to perform real-time authentication of subscriber mobile stations (radios) and infrastructure devices without need to transmit a secret authentication key.

1.2 AuC, PrC and AIE Introduction

This section provides an overview of the Authentication Centre (AuC) and Provisioning Centre (PrC) components installed in the DIMETRA system.

Infrastructure Keys are provisioned via the Key Variable Loader (KVL). Other keys and infrastructure data are distributed via TCP/IP network to infrastructure devices.

These devices are:

- Zone Controller (ZC)
- Motorola Transceiver System (MTS)

The PrC generates, stores, and tracks delivery of K and TM-SCK keys to the radios, using the Key Variable Loader (KVL) as a proxy to transport and confirm delivery. In addition, the PrC generates and exports a file containing K-REF pairs to the Authentication Centre (AuC).

The Key Variable Loader (KVL) is a secure “store-and-forward” device for transporting and provisioning keys from the PrC to radios and from the AuC to Zone Controllers and BTSs. The CryptR2 provides tamper proof key encryption services. It must be installed in the designated PrC workstation and in the AuC Server.

1.3 Enhanced Authentication Centre

Enhanced Authentication Centre (EAuC) combines Authentication Centre and Provisioning Centre in one application installed on the Core Server. It allows to simplify process of transferring keys from PrC to AuC without using external carriers.

IMPORTANT: This manual describes AuC related content. For PrC specific procedures see *Provisioning Centre (PrC) User Manual*.

1.4
Authentication Centre

This section describes the basic principles of what the AuC does and its infrastructure. After reading the contents of this section you should:

- Be familiar with the functions that the AuC performs.
- Have gained an understanding of what the AuC Client, AuC Server and AuC Database do.

1.4.1
What is the Authentication Centre?

The Authentication Centre (AuC) is a Windows-based, client/server application used to manage encryption keys for the DIMETRA radio system. The AuC generates, stores, distributes, and updates encryption keys used by the DIMETRA systems optional Authentication and Air Interface Encryption feature.

The AuC also maintains an external connection to the Key Variable Loader (KVL). The AuC external connection is hosted by the serial port on the Core Server, which is shared with the Zone Controller (ZC) application server. An iGAS menu is used to switch between the two applications. The KVL is connected either directly or using a modem and is used for non-encrypted key transfers from the AuC to each zone or MTS site entity.

The AuC client/server application utilizes a "three-tier" approach that distributes the software application into three separate, but dependent entities.

1.4.2
Authentication Centre Client

The Authentication Centre (AuC) Client application provides the user interface for system operators to perform key management operations. The AuC client is an application that provides a Microsoft Windows look and feel.

NOTE: The link between AuC Client and AuC Server is encrypted using SSL protocol with RSA certificates and AES128 encryption.

1.4.2.1
Automatic Detection of Network Problems

The AuC Client application is able to detect network problems. When a connection between the client and the server breaks down a Reconnecting dialog box appears. It may take up to one minute before it appears. In this way you can finish your work gracefully and fix the underlying network problem (if necessary).

The automatic reconnecting function is not supported after long-term disconnection or server reboot and in such cases a restart of the client is recommended.

1.4.3
Authentication Centre Server

The Authentication Centre (AuC) Server application provides the back-end processing services for the overall AuC application. These services include:

- Transaction and security management
- Database access and management
- Client/server communications

- Logging and auditing services
- External entity services (CryptR2, KVL, UCS, ZDS, ZC, MTS, UEM and AuC)

Authentication Centre server application running Windows 10 is deployed together with the AuC database and the AuC client either on the Primary Core Server or on a separate hardware platform.

1.4.4
Authentication Centre Database

The Authentication Centre (AuC) database stores key management data and key material for use by the Authentication Centre client/server application. The data stored in the AuC database is encrypted and decrypted using a master key stored in the AuC encryption device.

1.5
Implementing Your Security Policy

This section describes planning steps required to make effective use of the DIMETRA systems authentication and air interface encryption features.

1.5.1
Planning Your Steps

Before performing the implementation steps in the next section, answer the following basic security questions (Table 1: Security Planning Questions on page 29), which should help you make some important decisions in implementing your security policy.

Table 1: Security Planning Questions

Security Question	System Feature/Control
Will you allow security class 1 radios to operate on the system?	UCM System object
Will authentication be required by radios?	UCM System object
How often do you want to change keys?	AuC Key Scheduling
How many organizations that must be cryptographically separated are going to use the system ?	AuC CMG Configuration
What will be the source of imported keys used in the system?	AuC Key Database
Who will have access to the Authentication Centre (AuC)?	AuC User Management
What permissions should each AuC user have?	AuC User Management
What key variable loaders (KVLs) are allowed to communicate with the AuC?	AuC System Management
If a new entity is added to the system, do you want the entity to automatically receive keys from AuC?	AuC System Management
How will sensitive documents and key material media (such as CDs) be stored?	N/A
How do you want to handle possible key compromise via a lost or stolen subscriber unit?	N/A

1.5.2
Technical Implementation Steps

Once you have made decisions as to your security policy, consider the following technical activities required in implementing authentication and air interface encryption key management for the DIMETRA system. The technical activities mentioned below are dealt with in the Authentication, Encryption and Provisioning manual.

- Installing and configuring the AuC application
- Setting up AuC user accounts
- Setting up overall authentication and air interface encryption operating parameters
- Installing and configuring the PrC application
- Configuring radio and key variable loader (KVL) objects
- Distributing keys to system infrastructure and subscriber devices
- Implementing a centralized key management system
- Archiving and logging key management activities
- Dealing with compromised units

Chapter 2

AuC Client Interface Reference

This section provides a complete reference for the screens encountered in the AuC. The information is subdivided into Main Window and Secondary Window sections.

2.1 Main Window Structure

This section describes the components that make up the applications main window.

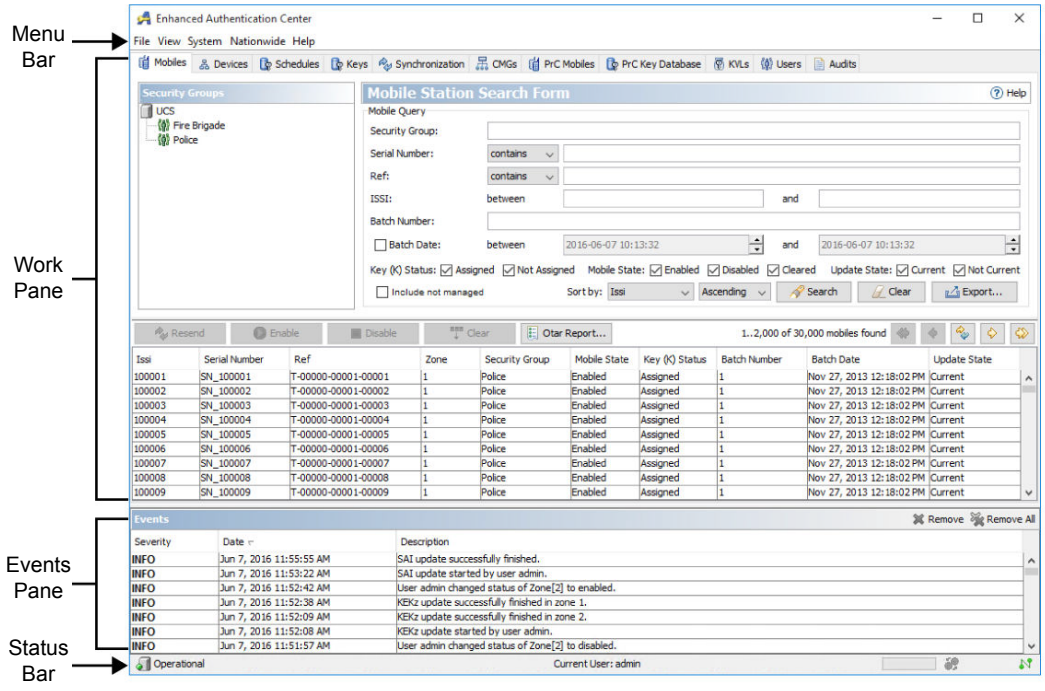
This section covers the following topics:

- Authentication Centre Main Window on page 31
- The Work Pane on page 32
- The Events Pane on page 32
- Status Bar on page 32
- The Menu Bar on page 33

2.1.1 Authentication Centre Main Window

The Authentication Centre (AuC) client main window allows you to view current status and perform tasks related to secure key management operations within the DIMETRA system.

Figure 1: The EAuC Main Window


Menu Bar
Work Pane
Events Pane
Status Bar
Enhanced Authentication Center
File View System Nationwide Help
Mobiles Devices Schedules Keys Synchronization CMGs PrC Mobiles PrC Key Database KVLs Users Audits
Security Groups
UCS
Fire Brigade
Police
Mobile Station Search Form
Mobile Query
Security Group:
Serial Number:
Ref:
ISSI:
Batch Number:
Batch Date:
Key (K) Status: Assigned Not Assigned
Mobile State: Enabled Disabled Cleared
Update State: Current Not Current
Include not managed
Sort by: Issi Ascending
Search Clear Export...
Resend Enable Disable Clear Otar Report...
1..2,000 of 30,000 mobiles found
Issi Serial Number Ref Zone Security Group Mobile State Key (K) Status Batch Number Batch Date Update State
Events
Remove Remove All
Severity Date Description
INFO Jun 7, 2016 11:55:55 AM SAI update successfully finished.
INFO Jun 7, 2016 11:53:22 AM SAI update started by user admin.
INFO Jun 7, 2016 11:52:42 AM User admin changed status of Zone[2] to enabled.
INFO Jun 7, 2016 11:52:38 AM KEKz update successfully finished in zone 1.
INFO Jun 7, 2016 11:52:09 AM KEKz update successfully finished in zone 2.
INFO Jun 7, 2016 11:52:08 AM KEKz update started by user admin.
INFO Jun 7, 2016 11:51:57 AM User admin changed status of Zone[2] to disabled.
Operational
Current User: admin

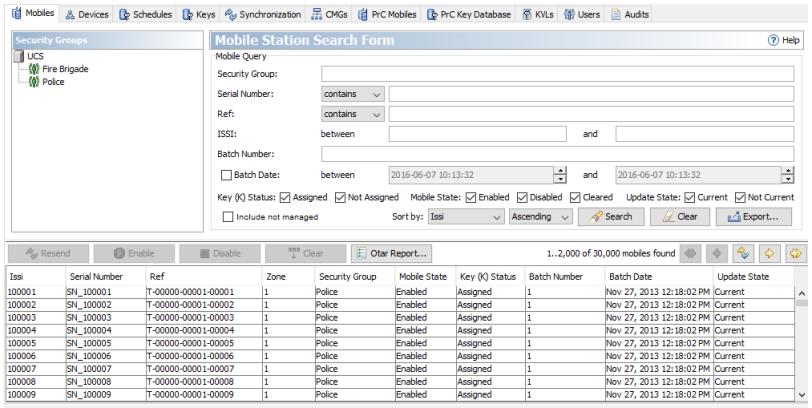
Maintaining a Microsoft Windows look and feel, the AuC main client window functions as the top-level container for the following user interface elements:

- The Work Pane on page 32
- The Events Pane on page 32
- Status Bar on page 32
- The Menu Bar on page 33

2.1.2
The Work Pane

The work pane – including tabs – is highlighted in the figure below.

Figure 2: The Work Pane – Encrypted AuC Example

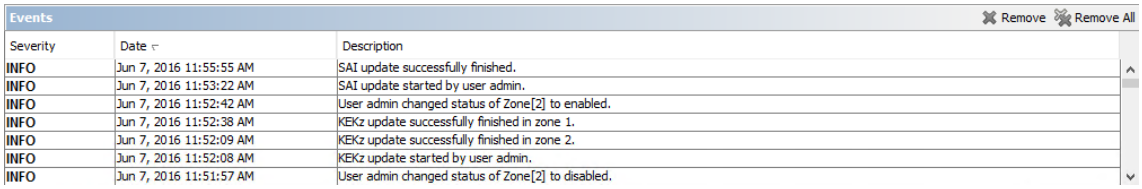


The work pane displays content corresponding to the task you are performing in the Authentication Centre (AuC) client. Acting as a container, the work pane allows you to switch among content selections using tabs. The content tabs that are selectable in the AuC main client window are listed in AuC Client Interface Reference on page 31.

2.1.3
The Events Pane

The events pane displays event information related to the actions you perform in the Authentication Centre (AuC) client.

Figure 3: The Events Pane

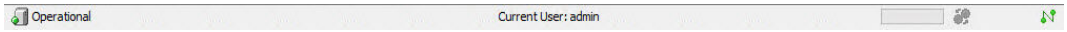

Events
Remove
Remove All
Severity
Date
Description
INFO Jun 7, 2016 11:55:55 AM SAI update successfully finished.
INFO Jun 7, 2016 11:53:22 AM SAI update started by user admin.
INFO Jun 7, 2016 11:52:42 AM User admin changed status of Zone[2] to enabled.
INFO Jun 7, 2016 11:52:38 AM KEKz update successfully finished in zone 1.
INFO Jun 7, 2016 11:52:09 AM KEKz update successfully finished in zone 2.
INFO Jun 7, 2016 11:52:08 AM KEKz update started by user admin.
INFO Jun 7, 2016 11:51:57 AM User admin changed status of Zone[2] to disabled.

2.1.4
Status Bar

The status bar provides information on the Authentication Centre (AuC) servers state, name of the clients current user, and various status icons.

The status bar is highlighted in the figure below.

Figure 4: Status Bar - Example



AuC state, AuC connection status and name of the user logged in appears in the status bar to the left, as shown above. The AuC Status icons to the left, report the conditions listed in the table below.

Table 2: Enhanced Authentication Centre (EAuC) States of Operation

Icon	AuC Server Operating State	Description
	Operational	Normal operating mode
	Out of Service	Non-operational mode. AuC client user can only perform the following tasks: • Loading a Master Key into an Encryption Device • All User Management tasks • Changing Authentication Centre operating state
	Database Restored	During Database Restored state only nationwide operations can be performed. Database Restored state is a sub-state of Out of Service state.
	Encryption Device Failure	State is shown when there is a problem with the CryptR2 configuration, for example if the Master Key is Not Loaded
	Database Failure	No connection between the AuC Server and the Database. Database Failure state is a sub-state of Out of Service state.

The EAuC Connection status icons to the right, report the conditions listed in the table below.

Table 3: Enhanced AuC Connection Status Icons

Icon	Description
	All required system devices (UCS and all ZDSs in the cluster) are connected to the AuC server.
	A system device (UCS or any of the ZDSs in the cluster) is not connected to the AuC server.
	A database backup is in progress.

2.1.5
The Menu Bar

The menu bar provides a list of commands from which you can choose to perform a task or navigate through the Authentication Centre (AuC) client application.

2.2
Main Window Elements

This section provides detailed reference information for each of the AuC applications main window elements.

2.2.1

AuC Comm Key (Communication Key)

Figure 5: AuC Comm Key (Communication Key) Display

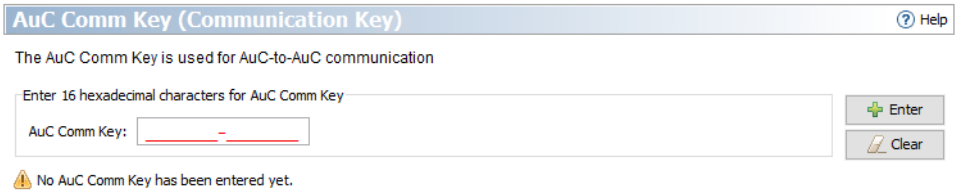

AuC Comm Key (Communication Key)
Help
The AuC Comm Key is used for AuC-to-AuC communication
Enter 16 hexadecimal characters for AuC Comm Key
AuC Comm Key:
Enter
Clear
No AuC Comm Key has been entered yet.

Table 4: Fields in the AuC Comm Key (Communication Key) Display

Field	Description
AuC Comm Key	The key consists of a 16 character hexadecimal key.
Status	Indicates whether an AuC Comm Key has been entered into the AuC. An AuC Comm Key can be entered multiple times with different values, but the key must be the same for all nationwide AuCs.

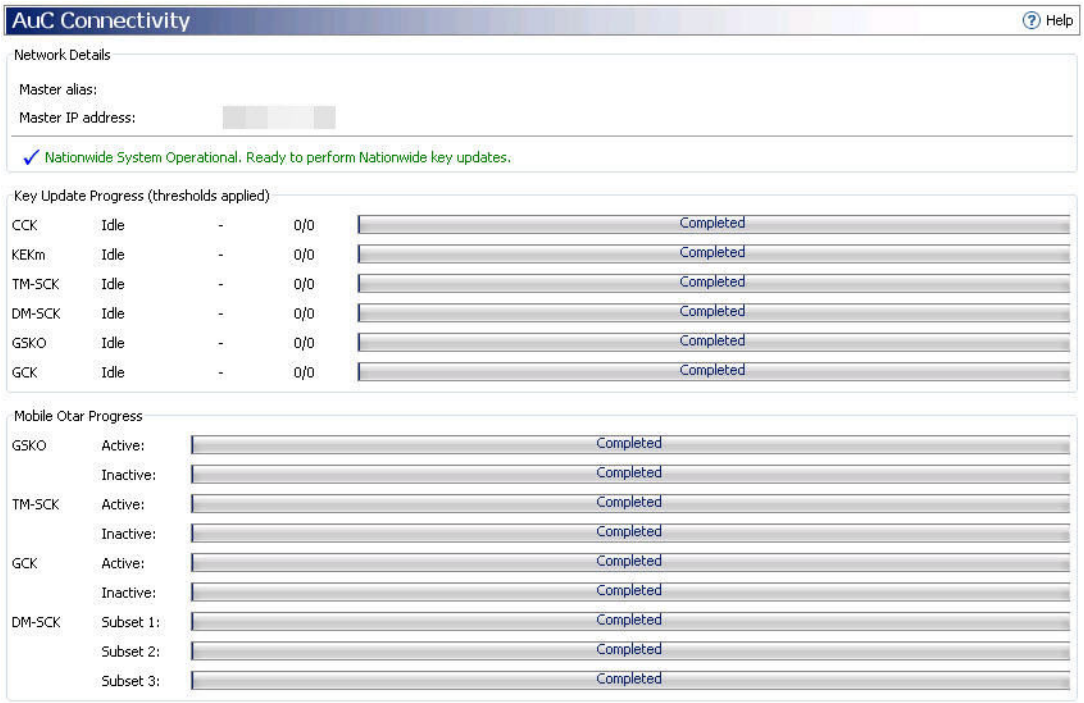
Table 5: Buttons in the AuC Comm Key (Communication Key) Display

Button	Action
Enter	Writes the AuC Comm Key to the server. The Enter button is only enabled when the AuC Comm Key is of the correct length.
Clear	Clears the field in the display. It does not erase the AuC Comm Key on the server.
Help	Launches the AuC online help window

2.2.2

AuC Connectivity

Figure 6: AuC Connectivity Display



The **AuC Connectivity** display provides information about the AuC server selected in the **AuC Net** window.

Table 6: Fields in the AuC Connectivity Information Display

Field	Values	Description
Server Alias	n/a	A user friendly description for selected AuC Server. **NOTE:** It is possible for different AuCs in a nationwide system to have the same alias, but this is not recommended.
Server ID	1 - 9 999 999	The selected AuCs server ID.
Server Version	n/a	Number of the AuC server application build.
Status	Connected	The selected AuC server is actively connected to the AuC network.
	Disconnected	Selected AuC server is not connected to the AuC network.
	Connecting...	The selected AuC server is connecting to the AuC network.
Nationwide Role	Master	Selected AuC server is a nationwide master.
	Slave	Selected AuC server is a nationwide slave.
	Expected Slave	Selected AuC server has been set on the Master AuC as Expected Slave AuC.

Field	Values	Description
IP Address	n/a	IP address of selected AuC server.
Information provided on Master AuC only:		
Information about key update lock on selected server. The name of the user who locked the key update, the date and reason of key update lock are displayed.		
Key update status for the CCK, SCK-TMO and System KEK for selected AuC server including following information for each key:		
Update Status	Idle	No key update in progress.
	Activate	Key update process is in the first stage.
	Update	Key update process is in the third stage.
	Refresh	Key update process is in the second stage (for System KEK update only).
	Unknown	Master AuC doesnt have complete information about key status on slaves.
Key Number	0 - 31	Number of the key that is sent out in current update stage (applies to the TM-SCK only). This information is displayed only when key update is in progress.
Key Version	1 - 65535	Version of the key that is sent out in current update stage. This information is displayed only when key update is in progress.
Key update progress	X/Y	Y - number of Zones/ Sites participating in key update.
		X - number of Zones/ Sites that already accepted key update.
Progress Indicator	n/a	Indicates the key update progress.

2.2.3
AuC Net

The **AuC Net** window displays the nationwide network tree. The icon and the information in brackets displayed next to each AuC Server listed in the **AuC Net** window represent its status.

Figure 7: AuC Net Pane Example

Table 7: AuC Server Status Information and Icons

Icon	Server Status	Description
	Connected	The AuC Server is actively connected to the AuC network.
	In-Service	The local AuC Server, that you are currently logged onto. The server is actively connected to the AuC network.
	Disconnected	The AuC Server is not connected to the AuC network.
	Out-Of-Service	The local AuC Server, that you are currently logged onto. The server is out of service.
	Expected	The AuC Server that is configured on the Master AuC as the Expected Slave AuC.
	Connected	The AuC Server is actively connected to the AuC network. The key updates are locked on this server.
	Restoring	The AuC server has been restored.
	Unknown	The AuC server IP address is unknown.

2.2.4 Audit Search and Purge Form

The **Audit Search Purge Form** window is shown below.

Figure 8: Audit Search Purge Form

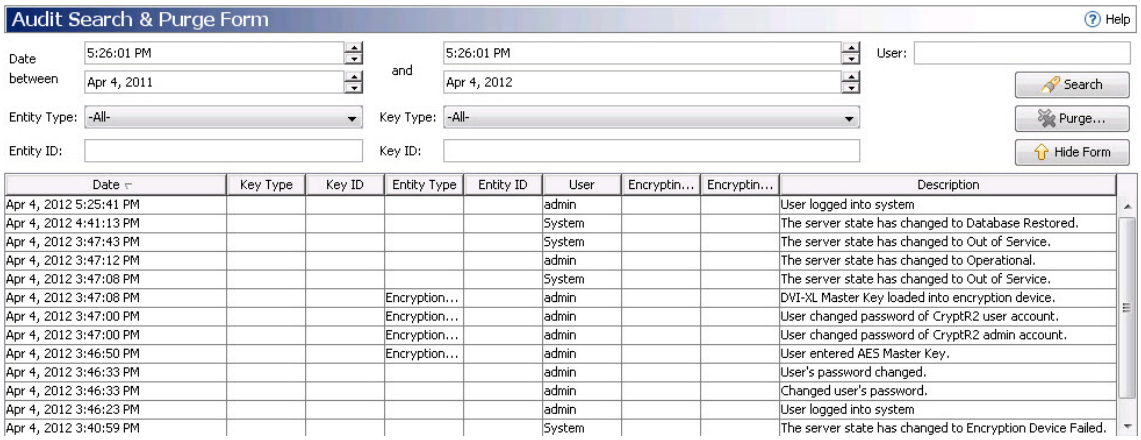

Audit Search & Purge Form
Help
Date between
5:26:01 PM
Apr 4, 2011
and
5:26:01 PM
Apr 4, 2012
User:
Search
Purge...
Hide Form
Entity Type:
-All-
Key Type:
-All-
Entity ID:
Key ID:
Date
Key Type
Key ID
Entity Type
Entity ID
User
Encryptin...
Encryptin...
Description
Apr 4, 2012 5:25:41 PM admin User logged into system
Apr 4, 2012 4:41:13 PM System The server state has changed to Database Restored.
Apr 4, 2012 3:47:43 PM System The server state has changed to Out of Service.
Apr 4, 2012 3:47:12 PM admin The server state has changed to Operational.
Apr 4, 2012 3:47:08 PM System The server state has changed to Out of Service.
Apr 4, 2012 3:47:08 PM Encryption... admin DVI-XL Master Key loaded into encryption device.
Apr 4, 2012 3:47:00 PM Encryption... admin User changed password of CryptR2 user account.
Apr 4, 2012 3:47:00 PM Encryption... admin User changed password of CryptR2 admin account.
Apr 4, 2012 3:46:50 PM Encryption... admin User entered AES Master Key.
Apr 4, 2012 3:46:33 PM admin User's password changed.
Apr 4, 2012 3:46:33 PM admin Changed user's password.
Apr 4, 2012 3:46:23 PM admin User logged into system
Apr 4, 2012 3:40:59 PM System The server state has changed to Encryption Device Failed.

Table 8: Fields in the Audit Search Purge Form display

Field	Description
Date between	Range of dates to search. Use spin boxes or manual entry to set beginning and ending time and date.
User	User login name to search
Entity Type	Type of entity to search. Use drop-down list box to select entity type.
Entity ID	ID of entity to search.
Key Type	Type of key to search. Use drop-down list box to search key type.

Field	Description
Key ID	ID of key to search.

Table 9: Buttons in the Audit Search Purge Form display

Button	Action
Search	Performs search using selected criteria. Results are listed in the Audit Trail Information list box.
Hide Form	Removes Audit Trail Search Criteria fields from window. Only displayed when fields are visible
Purge	Opens the Purge Audit Trail dialog box.
Show Search Purge Form	Shows Audit Trail Search Criteria fields in the window. Only displayed when fields are invisible.

2.2.4.1
Audit Trail Information Display

The fields presented in the Audit Trail information display are listed in the table below. By default, events are listed as they occurred (by Date). You can resort the listed events by clicking the column header. Clicking on a column header toggles the list items in forward and reverse order, respectively. A small triangle next to a column header indicates by which field the items are currently sorted.

Table 10: Fields in the Audit Trail Information display

Field	Description
Date	Date of event.
Key Type	Type of delivered key: Authentication Material, System KEK, Zone KEK, SCK, CCK.
Key ID	ID of delivered key (assigned by AuC).
Entity Type	Type of entity: Zone, BTS site, radio, KVL.
Entity ID	ID of entity (assigned by AuC).
User	Login name of user performing event task.
Encrypting Key Type	Type of sealing key (key used to encrypt delivered key for transport).
Encrypting Key ID	ID of sealing key (assigned by AuC).
Description	Description of event

2.2.5
CMGs Tree View Display

The **CMGs** tree view displays the CMG hierarchy. At the top of the tree, the **Unassigned MSs (Default CMG)** node is displayed. This is a pseudo CMG that contains all ISSI ranges that are not assigned to any CMGs.

The (valid) CMGs can be displayed underneath. The CMGs can contain TMO and DMO operational groups. The icons displayed next to operational group names indicate if a group is a common group (that is, is shared by more than one CMG) or not, as described in table below

Table 11: Operational Group Icons

Icon	Description
Blue icon	The operational group is contained by one CMG only.
Green icon	The operationl group is a common group - is contained by more than one CMG.

At the bottom of the tree, the **Orphan Operational Groups** node can be displayed. This a pseudo CMG that contains all TMO and DMO operational groups that are not contained by any CMGs. (This can happen only during import, when the mapping between operational groups and GSSI ranges is imported, but not the mapping between CMGs and the groups.)

Table 12: Buttons in the CMG Tree View Display

Button	Description
Sort by name	Sorts operational groups by name.
Sort by GCKN/KAGN	Sorts operational groups by GCKN/KAGN.
Create CMG	Creates a new CMG.
Remove CMG	Removes the selected CMG.
Create Operational Group	Creates a new operational group.
Remove Operational Group	Removes the selected operational group.
Auto Assign GCKNs	Automatically assigns GCKNs to TMO operational groups.
Auto Assign KAGNs	Automatically assigns KAGNs to DMO operational groups.
Enable / Disable Configu-ration	Enables / disables the CMG configuration.

2.2.6
CMG Information

Table 13: Fields in the CMG Information Display

Field	Description
Name	Name of the CMG.
Active	Status of the CMG - enabled or disabled.
Start	Start of a ISSI range.
End	End of a ISSI range.

Table 14: Buttons in the CMG Information Display

Button	Description
Edit CMGs	Opens the Edited Hierarchy tab allowing to update the enabled CMG configuration.
Apply Updates	Applies the updates performed on the enabled CMG configuration using the Edited Hierarchy tab.

Button	Description
Cancel	Cancels the updates performed on the enabled CMG configuration using the Edited Hierarchy tab.
Create ISSI Range	Creates a new ISSI range.
Remove ISSI Range	Removes the selected ISSI range.

2.2.7 DDK (DIMETRA Distribution Key)

Table 15: Fields in the DDK Information display

Field	Description
DDK	Entry of DDK key value. The DDK key is a 32-digit hexadecimal value.
Status	Status of DDK in AuC (entered or not entered in the AuC).

Table 16: Buttons in the DDK Information display

Button	Action
Enter	Commits DDK key entry (DDK field) to AuC database. Enabled only when proper DDK key is entered in DDK field.
Clear	Clears DDK field entry.
Help	Launches the AuC online help window.

2.2.8 BTS Site Information

Table 17: Fields in the BTS Site Information display

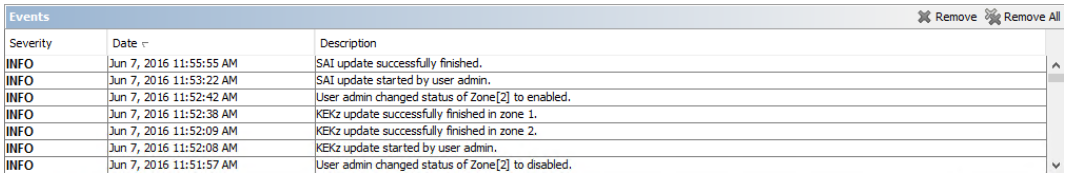
Field	Description
Status	Current setting for Key Updates (enabled or disabled).
CCK	Tabular display of the Common Cipher Key (CCK) version and status information for the selected BTS site entity.
Ki	Tabular display of infrastructure key (Ki) information and status for the BTS site entity.
TM-SCK	Tabular display of static cipher key-trunked mode operation (SCK-TMO) key information and status for the BTS site entity.
Zone KEK	Tabular display of zone key encryption key (KEKz) information and status for the BTS site entity.
OTAR keys	Tabular display of OTAR status for the BTS site entity.
MGCK	Tabular display of modified group cipher key (MGCK) information and status for the BTS site entity.

Table 18: Buttons in the BTS Site Information display

Button	Action
Enable	Enables key updates for the BTS site. Only displayed when key updates are disabled (see Status field).
Disable	Disables key updates for the BTS site. Only displayed when key updates are enabled (see Status field).
Resend	Redistributes current keys (except for Ki) for BTS site entities.
Refresh Ki	Redistributes the existing infrastructure key (Ki) for BTS site entities.
Update Ki	Assigns a new infrastructure key (Ki) for BTS site entities.
Help	Launches the AuC online help window.

2.2.9 Events Information

Figure 9: Events Pane


Events
Remove
Remove All
Severity
Date
Description
INFO Jun 7, 2016 11:55:55 AM SAI update successfully finished.
INFO Jun 7, 2016 11:53:22 AM SAI update started by user admin.
INFO Jun 7, 2016 11:52:42 AM User admin changed status of Zone[2] to enabled.
INFO Jun 7, 2016 11:52:38 AM KEKz update successfully finished in zone 1.
INFO Jun 7, 2016 11:52:09 AM KEKz update successfully finished in zone 2.
INFO Jun 7, 2016 11:52:08 AM KEKz update started by user admin.
INFO Jun 7, 2016 11:51:57 AM User admin changed status of Zone[2] to disabled.

The fields presented in the Events Information display are listed below. By default, events are listed as they occur (by Date). You can resort the listed events by clicking the column header. Clicking on a column header toggles the list items in forward and reverse order, respectively. A small triangle next to the column header indicates by which field the items are currently sorted.

Table 19: Fields in the Events Information Display

Field	Description
Severity	Severity of event.
Description	Description of event.
Date	Date of event.

Table 20: Buttons in the Events Information Display

Button	Action
Remove	Removes highlighted events from display.
Remove All	Removes all events from display.

2.2.10 AuC Connectivity Information

The **AuC Connectivity** window displays the summary of the nationwide network status.

Figure 10: AuC Connectivity Information Display

Table 21: Fields in the AuC Connectivity Information Display

Field	Values	Description
Master Alias	n/a	A user friendly description for Master AuC Server. **NOTE:** It is possible for different AuCs in a nationwide system to have the same alias, but this is not recommended.
Master IP Address	n/a	IP address of Master AuC server.
Expected Slave	n/a	IP address of Expected Slave AuC server set on Master AuC.
Summary of the key update status for the CCK, SCK-TMO and System KEK for the whole nationwide AuC network including following information for each key:		
Update Status	Idle	No key update in progress.
	Activate	Key update process is in the first stage.
	Update	Key update process is in the third stage.
	Refresh	Key update process is in the second stage (for System KEK update only).
	Unknown	Master AuC doesnt have complete information about key status on slaves.
Key Number	0 - 31	Number of the key that is sent out in current update stage (applies to the SCK-TMO only). This information is displayed only when key update is in progress.
Key version	1 - 65535	Version of the key that is sent out in current update stage. This information is displayed only when key update is in progress.
Key update progress	X/Y	Y - number of all Zones/ Sites in the nationwide network participating in key update.
		X - number of Zones/ Sites in the nationwide network that already accepted key update.
Progress Indicator	n/a	Indicates the key update progress.
Nationwide Status	Nationwide network currently establishing connectivity	AuCs are attempting to connect to the nationwide system (during upgrade process only).
	Nationwide System Operational. Ready to	AuCs are connected to the nationwide system. Key updates can now be performed.

Field	Values	Description
	perform nationwide key updates.	
	Need all listed AuCs connected before able to perform nationwide operations.	Either it was not possible to connect all of the AuCs or one or more of them lost connectivity after achieving it. The AuC(s) that could not be connected will be indicated in the **AuC Net** window.
	Single AuC configuration.	The AuC is not connected to a nationwide system.

2.2.11
K-REF Pairs

Table 22: Fields in the K-REF Pairs Information Display

Field	Description
K	Entry of actual authentication key (K) for the radio. The K key is a 32-digit hexadecimal value.
Ref: S	Entry of actual reference number for the radio. The reference number will be either the Subscriber Identification Module (SIM) or TETRA Equipment Identifier (TEI) (based on selection of SIM or TEI option button).
SIM	Select option button to designate the Ref field as a SIM entry.
TEI	Select option button to designate the Ref field as a TEI entry.
Unmatched K-Refs	A list of Refs for which a K-Ref pair is defined in the AuC but no matching Individual TETRA Subscriber Identity (ITSI) Ref pair is found. These items are listed in alphanumeric order. Their batch date and batch number are also shown. These are set at the time of their creation. If a K-Ref pair is entered manually, the batch number will be blank.
Ref	Allows you to narrow the search criteria for the unmatched K-Ref pairs. You can narrow the search criteria by selecting one of the options listed in the drop-down box: **contains**, **equals** or **begins with**.
Batch Number	Allows you to narrow the search criteria for the unmatched K-Ref pairs. Using this option allows you to list only the K-Ref pairs with the selected Batch Number.
Batch Date	Allows you to narrow the time frames for searched K-Ref pairs.
Sort by	The drop-down boxes allow you to sort the listed unmatched K-Ref pairs using listed options: **Ref**, **Batch Number**, **Batch Date**, "**Ascending**", "**Descending**".

Table 23: Buttons in the K-REF Pairs Information Display

Button	Action
Enter	Commits K and Ref entries to AuC database. The button is disabled until the proper K and Ref entries are made in corresponding fields.

Button	Action
	After selecting this button, the Unmatched K-REFs list box is automatically refreshed. If the Ref of the new K-Ref entered already exists in the AuC, a confirmation prompt appears.
Clear	Clears K and Ref field entries.
Delete	Removes highlighted unmatched K-REF pair from the AuC database.
Delete All	Removes all unmatched K-REF pairs from the AuC database.
Export Report	Generates a report of unmatched K-Ref pairs.
First Page	Shows the first batch of unmatched K-Ref Pairs.
Previous Page	Shows the previous batch of Unmatched K-Ref Pairs.
Refresh	Refreshes listings in Unmatched K-REFs list box.
Next Page	Shows the next batch of unmatched K-Ref Pairs.
Last Page	Shows the last batch of unmatched K-Ref Pairs
Help	Launches the AuC online help window.

2.2.12 Transfer KRefs

Table 24: Fields in the Transfer KRefs Window

Field	Description
Overwritten	After selecting this option and pressing continue all the previously filtered KRef pairs will be transferred from the PrC to AuC. KRef pairs already existing in the AuC database will be overwritten.
Skipped	After selecting this option and pressing continue only the previously filtered KRef pairs that do not exist in the AuC database will be transferred from the PrC to AuC. KRef pairs already existing in the AuC database will not be transferred.
Custom	After selecting this option a K-Refs to overwrite window appears listing all the previously filtered keys for which Refs exist in both AuC and PrC. You are able to select K-Refs that will be overwritten. Then when you press the Continue button, K-Refs selected in the Custom table will be transferred (overwriting existing ones in AuC) and K-Refs not existing in AuC (previously filtered) will be transferred either.

2.2.13
Key Database Selection

Table 25: Fields in the Key Database Selection Display

Field	Description
K-Ref Pairs	Places the K-REF Pairs Information display in the work pane.
SCK-Trunked Mode Operation	Places the SCK-TMO Information display in the work pane.
DDK (DIMETRA Distribution Key)	Places the DDK Information display in the work pane.
AuC Comm Key (Communication Key)	Places the AuC Comm Information display in the work pane.
Raw Keys Management	Places the Raw Keys Management display in the work pane.

2.2.14
Key Schedule Information

The **Key Schedule Information** window displays information corresponding with the key type selected in the **Key Schedule** window.

Figure 11: Key Schedule Information Display - Example

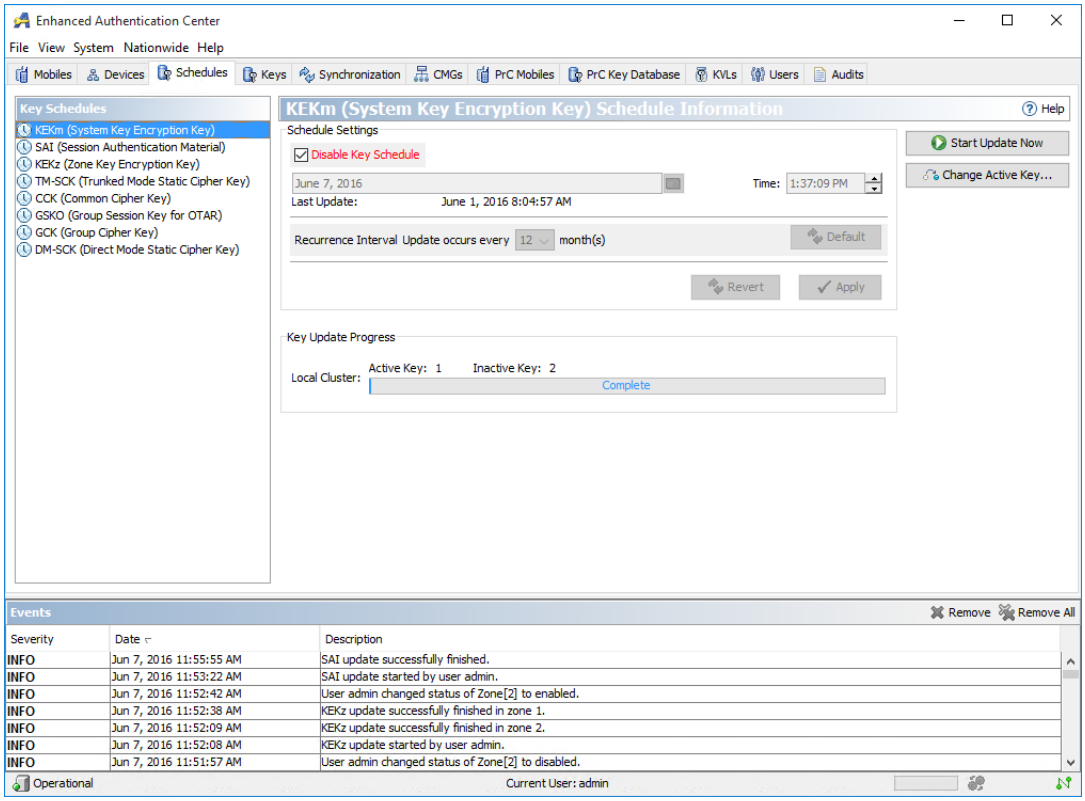

Enhanced Authentication Center
File View System Nationwide Help
Mobiles Devices Schedules Keys Synchronization CMGs PrC Mobiles PrC Key Database KVLs Users Audits
Key Schedules
KEKm (System Key Encryption Key)
SAI (Session Authentication Material)
KEKz (Zone Key Encryption Key)
TM-SCK (Trunked Mode Static Cipher Key)
CCK (Common Cipher Key)
GSKO (Group Session Key for OTAR)
GCK (Group Cipher Key)
DM-SCK (Direct Mode Static Cipher Key)
KEKm (System Key Encryption Key) Schedule Information
Help
Schedule Settings
Disable Key Schedule
June 7, 2016
Time: 1:37:09 PM
Last Update: June 1, 2016 8:04:57 AM
Start Update Now
Change Active Key...
Recurrence Interval Update occurs every 12 month(s)
Default
Revert
Apply
Key Update Progress
Local Cluster: Active Key: 1 Inactive Key: 2
Complete
Events
Remove
Remove All
Severity
Date
Description
INFO Jun 7, 2016 11:55:55 AM SAI update successfully finished.
INFO Jun 7, 2016 11:53:22 AM SAI update started by user admin.
INFO Jun 7, 2016 11:52:42 AM User admin changed status of Zone[2] to enabled.
INFO Jun 7, 2016 11:52:38 AM KEKz update successfully finished in zone 1.
INFO Jun 7, 2016 11:52:09 AM KEKz update successfully finished in zone 2.
INFO Jun 7, 2016 11:52:08 AM KEKz update started by user admin.
INFO Jun 7, 2016 11:51:57 AM User admin changed status of Zone[2] to disabled.
Operational
Current User: admin

Table 26: Fields in the Key Schedule Information Display

Field	Description
Last Update	Shows the date and time when the last update was started.
Recurrence Interval	Shows the interval for the updates. The interval is shown in months or days, depending on the key type.
Key Update Progress	Progress bars showing key update progress in local cluster. Depending on the key type, there can be either one progress bar showing overall progress for the cluster or separate progress bars for each zone.

Table 27: Buttons in the Key Schedule Information Display

Button	Action
Start Update Now	Forces an update to start immediately. A manual update has no impact on the date and time of the next scheduled update.
Help	Launches the AuC online help window.

2.2.15 Key Schedules Selection

Table 28: Fields in the Key Update Selection Display

Field	Description
KEKm	Places Key Schedule Information display in the work pane for System Key Encryption Key (KEKm).
SAI	Places Key Schedule Information display in the work pane for Secure Authentication Material (SAI).
KEKz	Places Key Schedule Information display in the work pane for Zone Key Encryption Key (KEKz).
CCK	Places Key Schedule Information display in the work pane for Common Cipher Key (CCK).
TM-SCK	Places Key Schedule Information display in the work pane for Static Cipher Key (SCK-TMO).
GSKO	Places Key Schedule Information display in the work pane for Group Session Key for OTAR (GSKO).
GCK	Places Key Schedule Information display in the work pane for Group Cipher Key (GCK).
DM-SCK	Places Key Schedule Information display in the work pane for Direct Mode Static Cipher Key (DM-SCK).

2.2.16 Key Status Tree View

The colored icons displayed next to each zone and site represent the entity's current key status.

Table 29: Key Status Icons (Zones and sites)

Icon	Description
	Requires Attention: The entity is missing both infrastructure keys (Ki), the infrastructure key (Ki) has been improperly provisioned or equipment failure occurred.
	Requires Attention: The entity is missing both infrastructure keys (Ki), the infrastructure key (Ki) has been improperly provisioned or equipment failure occurred and the entity is disabled from receiving key updates.
	Requires Attention: The entity is missing both infrastructure keys (Ki), the infrastructure key (Ki) has been improperly provisioned or equipment failure occurred and the entity is disconnected from the Zone Manager (ZM) (for zone entities only).
	Entity is not current: For Ki key - Entity may have current keys (is synchronized and able to communicate) but there could be update or refresh operation in progress (unfinished). For other keys: The entity no longer has the most current key version.
	Entity is not current and disabled: Entity may have current keys (is synchronized and able to communicate) but there could be unfinished update operation in progress (for example Ki update) and the key updates on the entity have been disabled.
	Entity is not current and disconnected: Entity may have current keys (is synchronized and able to communicate) but there could be unfinished update operation in progress (for example Ki update) and is disconnected from the Zone Manager (ZM) (for zone entities only).
	Entity is current The entity has the most current key version.
	Entity is current The entity has the most current key version but the key updates on the entity have been disabled.
	Entity is current The entity has the most current key version but is disconnected from the Zone Manager (ZM) (for zone entities only).

2.2.17 KVL Information

Table 30: Fields in the KVL Information Display

Field	Description
Alias	Alias of KVL (obtained from User Configuration Server (UCS)).
ID	ID of KVL (obtained from User Configuration Server (UCS)).
Status	Current setting for KVL access to AuC (access allowed or locked out).

Table 31: Buttons in the KVL Information Display

Button	Action
Deny Access	Locks out KVL access to the AuC. Only displayed when KVL access to AuC is allowed (see Status field).

Button	Action
Allow Access	Allows KVL access to the AuC. Only displayed when KVL access to AuC is locked out (see Status field).
Assign New UKEK	Launches KVL UKEK Assignment Dialog Box.
Help	Launches the AuC online help window.

2.2.18 KVL Status List View

Table 32: Key Status Icons (KVLs)

Icon	Description
	Locked out from AuC connectivity.
	Unprovisioned in the AuC database (does not have a UKEK key).
	Provisioned in the AuC database.

2.2.19 Mapping Types Display

The Mapping Types Display shows the list of the current Mapping Types.

Table 33: Buttons in the Mapping Types Display

Button	Description
Import mappings into the selected configuration	Allows to importing mappings from a file.
Export mappings from the selected configuration	Allows to export the mappings to a file.

2.2.20 Mobile Stations List

The fields presented in the Mobile Stations List pane are listed below. By default, query results are listed by Serial Number. You can resort the listed items by clicking the column header. Clicking on a column header toggles the list items in forward and reverse order, respectively. A small triangle next to the column header indicates by which field the items are currently sorted.

Table 34: Fields in the Mobile Stations List Pane

Field	Description
Security Group Alias	Security group for the radio (obtained from User Configuration Server (UCS)).
Serial Number	Serial number for the radio (obtained from User Configuration Server (UCS)).

Field	Description
Ref	Reference number for the radio (obtained from User Configuration Server (UCS)). The reference number will be either the Subscriber Identity Module (SIM) or TETRA Equipment Identifier (TEI) number.
ISSI	Individual Short Subscriber ID (ISSI) for the radio (obtained from User Configuration Server (UCS)).
K Assigned	Indicates whether an authentication key (K) has been assigned to the radio (Yes or No).
Mobile State	State of the radio key update: • Enabled – search for radios with key updates enabled • Disabled – search for radios with key updates disabled • Cleared – search for radios which have key updates disabled manually by a user, but are allowed to register for this MS
Batch Date	Creation date of a K-REF pair assigned to the radio
Batch Number	Number assigned to a group of K-REF pairs during their creation time. If a K-REF pair was entered manually in the AuC client, then this field is blank.

Table 35: Buttons in the Mobile Stations List Pane

Button	Action
Resend	Launches an immediate update of authentication material for the radio(s) highlighted in the list box. This button is disabled until an MS is selected from the list box.
Enable	Enables authentication material key updates for the radio(s) highlighted in the list box. Only displayed when key updates are disabled (see Key Updates Disabled field). This button is disabled until an MS is selected from the list box.
Disable	Disables authentication material key updates for the radio(s) highlighted in the list box. Only displayed when key updates are enabled (see Key Updates Disabled field). This button is disabled until an MS is selected from the list box.
Clear	Disables authentication material key updates for the radio(s) highlighted in the list box , however specified MS is allowed to register without authentication. Displayed when key updates are enabled or disabled (see Key Updates Disabled field). This button is enabled until an MS does not belong to the Encrypted ISSI Range.
Otar Report	Opens Mobiles OTAR Keys Report dialog box.

2.2.21 Operational Group Information

Table 36: Fields in the Operational Group Information Display

Field	Description
Name	Name of the operational group.
CMG(s)	Names of the CMGs the operational group belong to.
GCKN / KAGN	GCKN / KAGN assigned to the operational group.
Start	Start of a GSSI range.
End	End of a GSSI range.

Table 37: Buttons in the Operational Group Information Display

Buttons	Description
Edit CMGs	Opens the Edited Hierarchy tab allowing to update the enabled CMG configuration.
Apply Updates	Applies the updates performed on the enabled CMG configuration using the Edited Hierarchy tab.
Cancel	Cancels the updates performed on the enabled CMG configuration using the Edited Hierarchy tab.
Create GSSI Range	Creates a new GSSI range.
Remove GSSI Range	Removes the selected GSSI range.

2.2.22 OTAR Progress Information

Table 38: Fields in the OTAR Progress Information Display

Field	Description
GSKO	Progress of OTAR of active and inactive GSKO summarized for all CMGs.
TM-SCK	Progress of OTAR of active and inactive TM-SCK summarized for all CMGs.
GCK	Progress of OTAR of active and inactive GCK summarized for all CMGs.
DM-SCK	Progress of OTAR of active and inactive DM-SCK summarized for all CMGs.

Table 39: Buttons in the OTAR Progress Information Display

Button	Description
Refresh	Refreshes the status of the keys.
Help	Launches the AuC online help window.

2.2.23

Mobile Station Search Form

Figure 12: Mobile Stations Search Form Pane

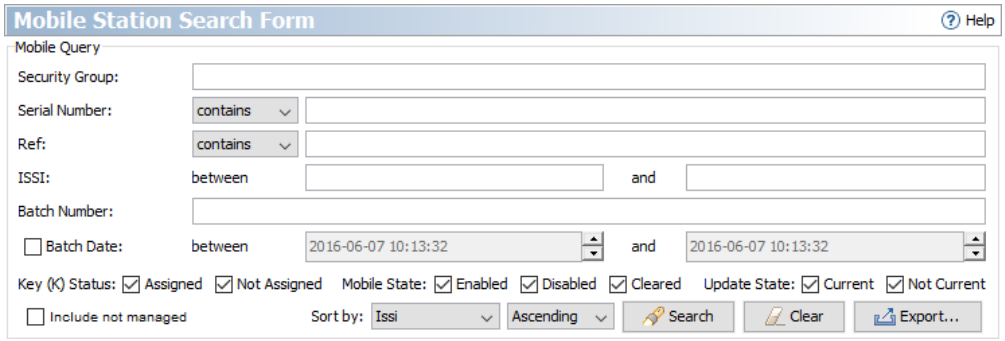


Table 40: Fields in the Mobile Stations Search Form Pane

Field	Description
Security Group	Security group to search. If field is left blank or contains "UCS", all security groups are searched
Serial Number	Serial number to search. Use drop-down list box to set condition of search using this field. If left blank, the field is not included in the search query.
Ref	Reference number to search. Use drop-down list box to set condition of search using this field. If left blank, the field is not included in the search query.
ISSI Between	Range of Individual Short Subscriber Identities (ISSIs) to search. Use both fields to type beginning and ending ISSIs, respectively. If blank; the leftmost field is set to 0 and rightmost field is set to 16,777,216.
Batch Number	Number assigned to a group of K-REF pairs when created. If left blank, the field is not included in the search query.
Batch Date	Range of K-REF pairs creation times to search. Use both fields to specify the beginning and end of a search period.
Secret Key (K) Status	Search for radios with or without an assigned authentication key (K) in the AuC database.
Mobile State	State of the radio key update: • Enabled – search for radios with key updates enabled • Disabled – search for radios with key updates disabled • Cleared – search for radios which have key updates disabled, but are allowed for registration
Include Not Managed	Includes unmanaged radios in the search.

Table 41: Buttons in the Mobile Stations Search Form Pane

Button	Action
Search	Performs search using selected criteria. Results are listed in Mobile Stations List Reference list box.

Button	Action
Export	Starts exporting radio information.
Clear	Clears entries from search criteria fields.

2.2.24
Mobiles OTAR Keys Reporting

Table 42: Fields in the Mobiles OTAR Key Report Display

Field	Description
Report Type	Report type group to run report against. Select the **Not Current mobiles** or the **Current mobiles** radio option.
Available active CMGs	Displays list of all active CMGs available. Use the down arrow button below the field to move CMGs to the **Selected CMGs** field.
Selected CMGs	Displays list of CMGs selected from the **Available active CMGs** list. To remove a CMG from the **Selected CMGs** list, select it and press the up arrow button.
Key Type	OTAR **Key Type** group to run report against. Select the Key type(s) to be included in the report.
Result Summary - Mobiles Tree	Displays a result summary for mobiles (current or not current, as selected in Report Type) per Key Type.
Result Summary - Statistics	Displays Mobiles OTAR keys statistics for mobiles (current or not current as selected in Report Type) for all OTAR Keys and for OTAR Keys selected in **Key Type**.

Table 43: Buttons in the Mobiles OTAR Keys Report Display

Button	Action
Run report	Performs a report
Sort by Keys	Sorts all mobiles in list on which Key Type they belong to.
Sort by Mobiles	Sorts all mobiles in list on which CMG they belong to.
Mobiles span list	Displays mobiles in span of 10. Unfold mobiles span in list to see mobiles belonging to that span.
All Mobiles list	Displays all mobiles in one list.
Export Report Summary	Starts exporting OTAR Keys information.

2.2.25
Raw Keys Management

Table 44: Fields in the Raw Keys Management Display

Field	Description
Pool Threshold	Specifies the threshold (the number of keys in the pool). When exceeded (i.e. the actual number of keys in the pool lower than threshold) generates a warning.
Number of keys in the pool	The number of raw keys of given type in the pool.

Table 45: Buttons in the Raw Keys Management Display

Button	Action
Generated by the encryption device	Generates raw keys of given type using the CryptR2.
Retrieved from the pool of imported keys	Uses raw keys of given type imported from files to the pool.
Delete All	Deletes all raw keys of given type from the pool.
Restore Defaults	Restores default settings.
Apply	Applies the changes in raw keys management.

2.2.26
SCK-Trunked Mode Operation Information

Table 46: Fields in the SCK-Trunked Mode Operation Information Display

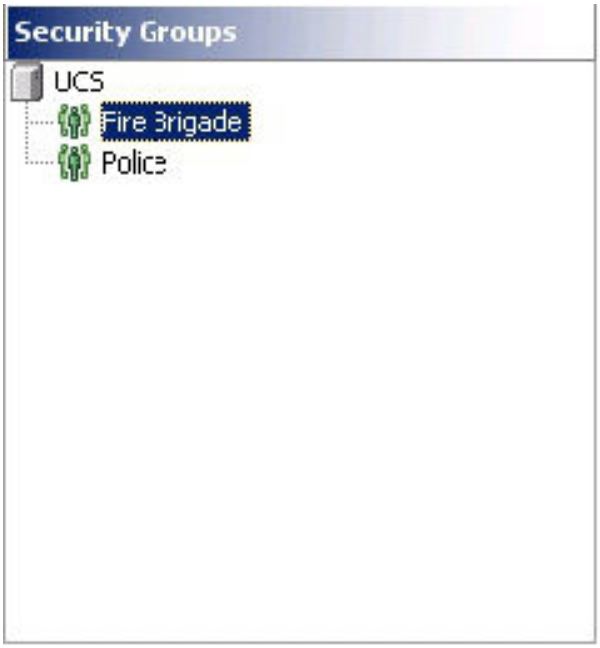
Field	Description
SCK Number	Number of SCK-TMO key slot
SCK Version	Version of SCK-TMO key in the slot
Active	Reflects the current and next active SCK-TMO keys. The following arrows reflect the current and next active SCK-TMO keys: currently active SCK-TMO key next active SCK-TMO key

Table 47: Buttons in the SCK-Trunked Mode Operation Information Display

Button	Action
Set 32 TMO / Set 2 TMO	Toggles between 32 and 2 TM-SCK mode.
Use Static Key / Use Raw Key	Toggles between imported and raw TM-SCK mode.
Help	Launches the AuC online help window.

2.2.27
Security Group Selection Tree View

Figure 13: Security Group Selection Tree View



Each security group stored in the Authentication Centre (AuC) database is listed in **Security Groups** pane.

2.2.28
UCS Information

Table 48: Fields in the UCS Information Display

Field	Description
UCS Status	Status of connection to User Configuration Server (UCS). Available values: • Disconnected • Disconnected – Invalid Version • Not Ready • Synchronizing • Connected
Connected since	Time of the last connection with UCS.
Disconnected since	Time of the last disconnection from UCS.

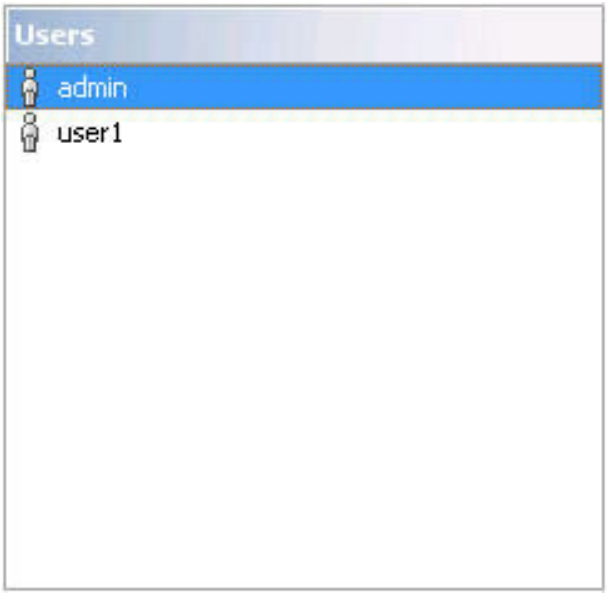
Table 49: Buttons in the UCS Information Display

Button	Action
Synchronize	Starts the full synchronization with UCS process.

Button	Action
Help	Launches the AuC online help window.

2.2.29
User Account Selection Tree View

Figure 14: User Account Selection Display



Each user account existing on the Authentication Centre (AuC) is listed.

2.2.30
User Information

Figure 15: User Information Display

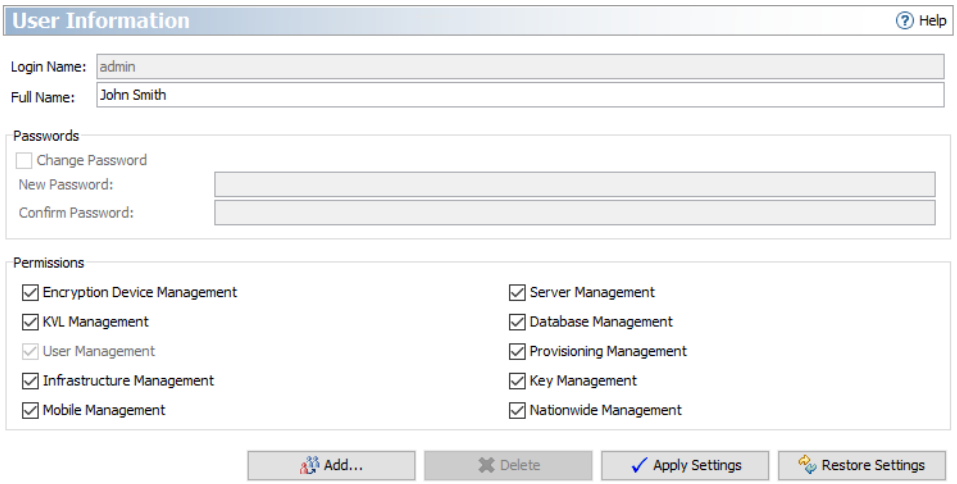


Table 50: Fields in the User Information Display

Field	Description
Login Name	Login name of AuC user. This field allows use of spaces. Login names are case sensitive. Users are not allowed to modify their login name.
Full Name	Full name of AuC user (Optional).
Change Password	Enables New Password and Confirm Password fields. **NOTE:** You cannot change your own password from this dialog box, when logged in as yourself, since User Management does not ask for the old password. To change your own password, see Changing a User Account Password on page 78.
New Password	New password for AuC user.
Confirm Password	New password for AuC user.
Permissions	Access permissions for user to AuC tasks. Use the check boxes to select which task categories the user can access and perform. A user with no permissions is able to only view entity information. See Table 51: Access Permissions for AuC Users on page 56 below.

Table 51: Access Permissions for AuC Users

Permission	Tasks
Encryption Device Management	Allows Encryption Device operations.
KVL Management	Allows the user to modify KVL records, change UKEK assignments, disable/enable a KVL from communication with the AuC, and modify the KVL port settings.
User Management	Allows all user management operations and audit trail purging.
Infrastructure Management	Allows disabling of zones and BTSs and all Zone/System KEK Key Schedule operations, including Ki Provisioning.
Mobile Management	Allows all MS operations and all Authentication Material Key Schedule operations.
Server Management	Allows **System> Preferences> Server Settings** operations.
Database Management	Allows all database operations.
Provisioning Management	Allows user to perform PrC specific actions.
Key Management	Allows entry of keys in Key Database, SCK-TMO and CCK operations, including Key Schedule operations.
Nationwide Management	Allows nationwide system connection operations under the Connections tab, CCK key updates, and entry of AuC Comm Key.

Table 52: Buttons in the User Information Display

Button	Action
Restore Settings	Restores user account information settings before current changes are committed to AuC database (i.e., to start over with modifications).

Button	Action
Apply Settings	Commits user account information settings to the AuC database.
Delete	Deletes user account from the AuC database.
Add	Launches the Add User Dialog Box.
Help	Launches the AuC online help window.

2.2.31
Zone Information

Table 53: Fields in the Zone Information Display

Field	Description
Device Id	Device identifier.
Alias	Device textual description.
Connection Status	The status of connection to the Zone Controller (ZC).
Key Status	The status of keys on the Zone Controller (ZC).
Mobiles	The status key updates of radios in the zone.
Ki	Tabular display of infrastructure key (Ki) information and status for the Zone Controller (ZC).
KEKm	Tabular display of system key encryption key (KEKm) information and status for the Zone Controller (ZC).
KEKz	Tabular display of zone key encryption key (KEKz) information and status for the Zone Controller (ZC).

Table 54: Buttons in the Zone Information Display

Button	Action
Enable / Disable	Enables / disables key updates for the Zone Controller (ZC).
Resend	Sends all key information to the Zone Controller (ZC).
Refresh Ki	Redistributes the existing infrastructure key (Ki) to the Zone Controller(s) (ZC).
Update Ki	Assigns a new infrastructure key (Ki) to the Zone Controller(s) (ZC).
Help	Launches the AuC online help window.

2.3
Secondary Window

This section provides detailed information of the AuC applications secondary windows.

2.3.1

Add User Dialog Box

Figure 16: Add User Dialog Box

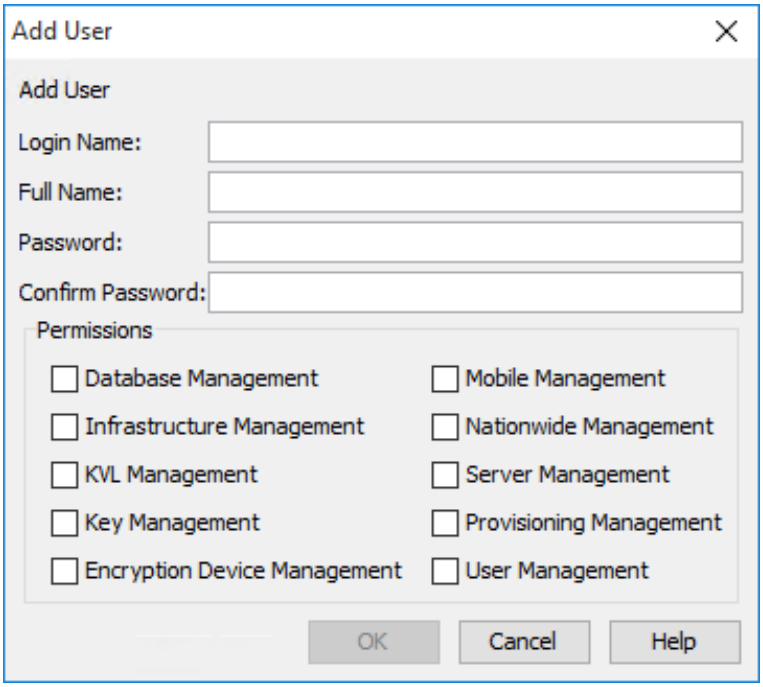


Table 55: Fields in the Add User Dialog Box

Field	Description
Login Name	Login name of AuC user.
Full Name	Full name of AuC user.
Password	New password of AuC user.
Confirm Password	New password of AuC user.
Permissions	Access permissions for user to AuC tasks. Use check boxes to select which task categories the user can access and perform. A summary of the tasks allowed for each checkbox is provided below.

Table 56: Access Permissions for AuC Users

Permission	Tasks
Encryption Device Management	Allows Encryption Device operations.
KVL Management	Allows the user to modify KVL records, change UKEK assignments, disable/enable a KVL from communication with the AuC, and modify the KVL port settings.
User Management	Allows all user management operations and audit trail purging.
Infrastructure Management	Allows disabling of zones and BTSs and all Zone/System KEK Key Schedule operations, including Ki Provisioning.

Permission	Tasks
Mobile Management	Allows all MS operations and all Authentication Material Key Schedule operations.
Server Management	Allows **System> Preferences> Server Settings** operations.
Database Management	Allows all database operations.
Provisioning Management	Allows user to perform PrC specific actions.
Key Management	Allows entry of keys in Key Database, SCK-TMO and CCK operations, including Key Schedule operations.
Nationwide Management	Allows nationwide system connection operations under the Connections tab, CCK key updates, and entry of AuC Comm Key.

Table 57: Buttons in the Add User Dialog Box

Button	Action
OK	Commits user account information settings to the AuC database.
Cancel	Cancels user account information settings without committing them to the AuC database.
Help	Launches the AuC online help window.

2.3.2
AuC Connection

Table 58: Fields in the AuC Connection Display

Field	Description
Enter the IP address of expected slave AuC	IP address for an AuC server that will be set by master AuC as the expected slave AuC.
Enter the IP address of master AuC	IP address of the master AuC that the local AuC will be connected to.

Table 59: Buttons in the AuC Connection Display

Button	Action
OK	Attempts to connect to the AuC using the IP address supplied.
Cancel	Closes the dialog box.

2.3.3
AuC Backup Dialog Box

Table 60: Fields in the AuC Backup Dialog Box

Field	Description
Backup in Progress	States whether an AuC database backup is currently in progress (yes or no). During backup, you will still be able to perform AuC operation. However, you will not be able to start a new backup, until the current backup is complete. Once backup is initiated, it cannot be cancelled.
Last Successful Backup	States when last AuC database backup occurred. The field displays **No backups performed yet** if no backup has been performed.
Next Scheduled Backup	States when next AuC database is scheduled to occur, even if backup schedules are disabled. The field displays **No schedule set yet** if no backup schedule has been set.
Backup Schedule Disabled	Checkbox to disable schedule backup of the AuC database. Disabling backup schedule is also possible while a backup is in progress. **NOTE:** Backups are not disabled until the **OK** button has been clicked, after **Backup Schedule Disabled** has been selected.
Path	Displays the current path for the for storing the AuC database backup file. The path is shown from the database servers perspective, not the clients Default is `C:\Motorola\AuC\ <version> \var\backup` where *<version>* is the version number.

Table 61: Buttons in the AuC Database Dialog Box

Button	Action
Modify Schedule	Launches the dialog box to schedule the AuC database backups.
Start Backup Now	Launches an immediate AuC database backup.
OK	Commits the AuC database backup settings.
Close	Closes the AuC Database dialog box.
Help	Launches the AuC online help window

2.3.4
Change Password Dialog Box

Table 62: Fields in the Change Password Dialog Box

Field	Description
User Name	Login name of AuC user (already populated).
Old Password	Entry for existing password.
New Password	Entry for new password.
Confirm New Password	Confirm entry for new password.

Table 63: Buttons in the Change Password Dialog Box

Button	Action
OK	Commits password change to AuC database.
Cancel	Cancels password change. **NOTE:** If the dialog was brought up after the login dialog, that is before the main screen is reached, and your password has expired, cancelling will force the client application to close.

2.3.5 Encryption Devices Dialog Box

Table 64: Fields in the Encryption Devices Dialog Box

Field	Description
Vendor	Name of the encryption device vendor.
Device Type	Type of encryption device.
Software Version	Version of software on encryption device
DVI-XL Master Key status	Indicates the state of the Master Key. The state can be **Loaded**, **Not loaded**, **Invalid** or **Unknown**. The **Invalid** state is created when a new Master Key is loaded, but does not match the one expected by the AuC.
AES Master Key status	Indicates the state of the Master Key. The state can be **Loaded**, **Not Entered on the server**, **Invalid**, **Not Available**. The **Invalid** state is created when a new Master Key is loaded. The **Not Available** state will be displayed when the DVI-XL Master Key was not loaded. Even if the AES Master Key is loaded AuC is not able to verify it while DVI-XL Master Key is not present.
User password status	Shows if password entered in the CryptR2 device matches password entered in the AuC.
Admin password status	Shows if password entered in the CryptR2 device matches password entered in the AuC.
Device Status	Status of the encryption device: **Working** or **Failed**. **NOTE:** The Master Key state has influence on the Encryption Device Status; when the Master Key state is not **Loaded** the Encryption Device Status is **Failed**.
Battery Level	Describes the battery level in the encryption device. The Level can be **Full**, **Dead** or **Unknown**.
Algorithms	List of required algorithms. When the algorithm is installed on the encryption device the corresponding checkbox is marked. **NOTE:** The completeness of installed algorithms has influence on the Encryption Device Status; when not all required algorithms are installed the Encryption Device Status is **Failed**.

Table 65: Buttons in the Encryption Devices Dialog Box

Button	Action
Enter AES Master Key	Opens dialog box that allows you to enter AES master key.
Load Master Key	Launches the Load Master Key wizard.
Enter password	Opens dialog box that allows you to enter User and admin password.
Validate	Validates passwords.
Request logs	Downloads the error logs from the CryptR2 device.
Close	Closes the Encryption Devices dialog box.
Help	Launches the AuC online help window.

2.3.6
Key Update Lock Details Information Box

Table 66: Field in the Key Update Lock Details Information Box

Field	Description
User	User who locked the key updates.
Date	Date of the key update lock operation.
Lock reason	Reason of locking the key updates.

Table 67: Buttons in the Key Update Lock Details Information Box

Button	Action
OK	Confirms the key update lock and its reason.
Cancel	Cancels the key update lock operation.

2.3.7
Key Update Lock Dialog Box

Table 68: Field in the Key Update Lock Dialog Box

Field	Description
Reason for locking key updates	Reason for locking key updates to be provided by the user.

Table 69: Buttons in the Key Update Lock Dialog Box

Button	Action
OK	Confirms the key update lock and its reason.
Cancel	Cancels the key update lock operation.

2.3.8
Key Report Contents Dialog Box

Table 70: Fields in the Key Report Contents Window

Field	Description

Zone keys	Allows key report to contain information about used keys for particular zone. In **Site keys** option you may select:
	• **Missing MGCKs** – info about missing Modified Group Cypher Keys
	• **CMG OTAR**
	  ○ **GCK currency**
	  ○ **TM SCK currency**
	  ○ **DM SCK currency**
	  ○ **DM SCK version**

AuC keys	Allows key report to contain information used in the whole system. You may select:
	• **GSKOs**
	  ○ **Dependent GCKs currency**
	  ○ **Dependent DM-SCKs currency**
	  ○ **TMSCK currency**
	• **GCK Groups**
	• **SCK Groups**

2.3.9
KVL UKEK Assignment Dialog Box

Table 71: Fields in the KVL UKEK Assignment Dialog Box

Field	Description
Enter new UKEK	Entry for unique key encryption key (UKEK) key value. The UKEK key is a 16-digit hexadecimal value.

Table 72: Buttons in the KVL UKEK Assignment Dialog Box

Button	Action
OK	Commits UKEK key to the AuC database. The button is disabled until 16 hexadecimal characters are entered in the Enter new UKEK field.
Cancel	Cancels UKEK key storage.

2.3.10
Login Dialog Box

Table 73: Fields in the Login Dialog Box

Field	Description
User Name	Login name for AuC user.
Password	Password for AuC user.
Server	AuC server address.

Table 74: Buttons in the Login Dialog Box

Button	Action
OK	Attempts to log the user in the AuC.
Exit	Cancels the login attempt
Details	Shows/hides the **Server** field

2.3.11
Miscellaneous Settings

Table 75: Fields Shown in the Preferences Dialog Box when the Miscellaneous Entity is Selected

Field	Description
Stop box synchronization during nationwide CMG operation	Prevents box synchronization during nationwide CMG operations.

Table 76: Buttons Shown in the Preferences Dialog Box when the Miscellaneous Entity is Selected

Button	Action
OK	Commits miscellaneous settings to AuC database
Cancel	Closes Settings dialog box.
Help	Launches the AuC online help window

2.3.12
Server Settings

Table 77: Fields Shown in the Preferences Dialog Box when Server Settings are Selected

Field	Description
Server ID	Entry for server) ID. This ID is necessary for the KVL and AuC to communicate effectively. If the AuC ID is not the ID expected by the KVL, the KVL will disconnect.

Field	Description
Server Alias	A user-friendly name (alias) for the server. The maximum length is 20 characters. There is no initial alias value.
Debug Log Enabled	Allows a debug log to be maintained on the server.

Table 78: Buttons Shown in the Preferences Dialog Box when Server Settings are Selected

Button	Action
OK	Commits miscellaneous settings to AuC database
Cancel	Closes Settings dialog box.
Help	Launches the AuC online help window

2.3.13
Port Settings

Table 79: Fields Shown in the Preferences Dialog Box when the Port Settings Entity is Selected

Field	Description
Port	AuC hardware port used to communicate with KVLs. Use drop-down list box to select port. After selection, the ports current settings are displayed in the dialog box.
Bit Rate	Bit rate for KVL communication port. Use drop-down list box to select bit rate.
Initialization String	Initialization string used for modem connection to KVL. This field is disabled when the Connection Type field is set to "Direct".
Connection	Type of connection used to communicate with KVL. Use options buttons to select the connection type: • **Direct** for cable connection • **Modem** for dialup connection
Type	Type of the application.

Table 80: Buttons Shown in the Preferences Dialog Box when the Port Settings Entity is Selected

Button	Action
Restore Default Settings	Resets KVL port settings to the AuC default settings.
OK	Commits KVL port settings to AuC database.
Cancel	Closes dialog box without changes being applied.
Help	Launches the AuC online help window.

2.3.14
Purge Audit Trail Dialog Box

Table 81: Fields in the Purge Audit Trail Dialog Box

Button	Description
Calendar button	Specifies number a particular date for audit trail data to keep in the AuC database (all data exceeding this setting will be archived to a file on the server). **IMPORTANT:** Setting the date of a purge to 10-OCT-2018 means that purge is performed for all audits up to and including October 10, 2018.

Table 82: Buttons in the Purge Audit Trail Dialog Box

Button	Action
Begin Purge	Launches the process of removing audit trail data from the AuC database.
Cancel	Cancels selection and closes dialog box.

2.3.15
SAI Cache Settings

Table 83: Fields Shown in the Preferences Dialog Box when the SAI Cache Entity is Selected

Field	Description
Active SAI in Cache	Number of SAI in cache for active KEKm.
Future SAI in Cache	Number of SAI in cache for inactive KEKm.

Table 84: Buttons Shown in the Preferences Dialog Box when the SAI Cache Entity is Selected

Button	Action
Fill	Fills the SAI cache with SAI for all mobiles.
Clear	Clears the SAI cache.
Auto Cache Population	If selected, every 15 minutes SAI keys are being generated for mobiles which do not have SAI keys in their cache. The maximum of 1000 keys can be generated at one time.
Refresh	Refreshes the displayed numbers of active and inactive SAI in cache.
OK	Commits settings to AuC database.
Cancel	Cancels the selection and closes Settings dialog box.
Help	Launches the AuC online help window.

2.3.16
SCK-TMO Modify Dialog Box

NOTE: A modified slot is not automatically distributed throughout the DIMETRA system until the slot is selected as the next active slot as part of a scheduled or manual update.

Table 85: Fields in the SCK-TMO Modify Dialog Box

Field	Description
Key Value	Entry for SCK-TMO key value. The SCK-TMO key is a 20-digit hexadecimal value.
Key Version	Version of SCK-TMO key.

Table 86: Buttons in the SCK-TMO Modify Dialog Box

Button	Action
OK	Commits entry to the AuC database.
Cancel	Cancels entry and closes dialog box.

2.3.17
User Settings

Table 87: Fields Shown in the Preferences Dialog Box when the User Settings Entity is Selected

Field	Description
Password Requirements:	The default settings can be configured according to the following limitations.
Maximum Length	The maximum number of characters allowed for a password. Maximum length: 20 characters.
Minimum Length	The minimum number of characters allowed for a password. Minimum length: 3 characters.
Passwords must contain at least one digit	When selected, the password must contain at least one digit.
Interval of days until passwords expire	Period of days after which a user will be required to change their password during log in. Minimum: 0 days, which means next login. Maximum: 100 days.
Username Requirements:	
Maximum Length	The maximum number of characters allowed for a user name Maximum: 20 characters.
Minimum Length	The minimum number of characters allowed for a user name. Minimum: 4 characters.

Table 88: Buttons Shown in the Preferences Dialog Box when the User Settings Entity is Selected

Button	Action
Restore Settings	Restores the applications default user settings.
OK	Commits user settings to AuC database.
Cancel	Cancels the selection and closes Settings dialog box.
Help	Launches the AuC online help window.

2.3.18 Thresholds Settings

Table 89: Fields Shown in the Preferences Dialog Box when the Thresholds Entity is Selected

Field	Description
GSKO OTAR threshold:	
GSKO OTAR threshold	The percentage of mobiles required to confirm • inactive GSKO prior to GSKO activation • active GSKO prior to OTAR AIE key activation
MS OTAR threshold:	
GCK OTAR threshold	The percentage of mobiles required to confirm inactive OTAR AIE key prior to GCK key configuration.
TM OTAR threshold	The percentage of mobiles required to confirm inactive OTAR AIE key prior to TM SCK key activation.
DM OTAR threshold	The percentage of mobiles required to confirm inactive OTAR AIE key prior to DM SCK key activation.
Site update threshold:	
CCK update threshold	The percentage of sites with current AIE key required to start and proceed with CCK key update.
GCK update threshold	The percentage of sites with current AIE key required to start and proceed with GCK key update.
DM SCK update threshold	The percentage of sites with current AIE key required to start and proceed with DM SCK key update.

Table 90: Buttons Shown in the Preferences Dialog Box when the Thresholds Entity is Selected

Button	Action
OK	Commits thresholds settings to AuC database.
Cancel	Cancels the selection and closes Settings dialog box.
Help	Launches the AuC online help window.

2.3.19
AuC Database Standby Manager Icon Descriptions

Table 91: AuC Server Standby Status Information Icon

Icon	Status	Description
	Synchronized	Active and standby databases are fully synchronized.
	Not Synchron-ized	The databases are not synchronized and setup of the standby AuC is in progress.
	Unknown	After start-up or standby synchronization service is unable to get the response regarding the synchronization status.
	Disconnected	Standby synchronization service is unable to get the connectivi-ty.
	Synchronizing	The synchronization of the recent data changes is in progress.

2.3.20
AuC Database Standby Manager Window Description

The **Database Standby Manager** window displays the AuC data redundancy status on the Standby and Active AuC. To check the status on Active or Standby AuC log onto the appropriate server and launch the Database Standby Manager.

If the **Database Standby Manager** shows that the databases of the active and standby AuC are fully synchronized (State: SYNCHRONIZED) only the upper part of the **Redundancy Status** pane is displayed in the **Database Standby Manager** window.

If the databases are in different than Synchronized stated additional information is displayed under Data currency, on the bottom of the **Redundancy Status** pane.

Table 92: Fields in the Database Standby Manager window

Field	Value	Description
Role	Active	Shows the role of the AuC machine.
	Standby	
Active/Standby host	See your DIME-TRA IP Plan.	Displays the IP address of the standby or active AuC.
State	Unknown	Displayed at start-up or if standby synchronization service is unable to get the response regarding the synchronization status.
	Disconnected	Displayed when standby synchronization service is unable to get the connectivity.
	Not Synchron-ized	Displayed if the databases are not synchronized and setup of the standby AuC is in progress.
	Synchronizing	Displayed if the synchronization of the recent data changes are in progress.
	Synchronized	Displayed when active and standby databases are fully synchronized.

Field	Value	Description
Last updated		Shows the time of the last redundancy status change or verification.
Last synchronized		Shows the time when standby and active were fully synchronized and state was “Synchronized”.
Last changes applied		Shows the time of the last change applied to the standby AuC as part of the synchronization process

Table 93: Buttons in the Database Standby Manager window

Button	Action
Show Details	Shows the Details pane.
Hide Details	Hides the Details pane.

2.4 Main Menu Items

Table 94: Main Menu Items

Menu Name	Submenu Name		Description
File	Import to AuC	SCK Keys	Initiates SCK keys import.
		K-Ref Pairs	Initiates K-Ref Pairs import.
		Raw Keys	Initiates raw keys import.
	Import To PrC	SCK Keys	Initiates SCK keys import.
		K Keys	Initiates K keys import.
	Export from PrC	K-Ref Keys	Initiates KRef keys export.
	Exit		Turns off the AuC Client.
View	AuC only		Shows AuC tabs only.
	PrC only		Shows PrC tabs only.
	Enhanced AuC		Shows all tabs.
System	Update Lock	Enable	Enables / disables key update lock.
		Details	Displays key update lock details.
	Backup		Opens the Backup dialog box.
	Key Report		Opens Key Report dialog box.
	Encryption Device		Opens the Encryption Devices dialog box.
	Change Password		Initiates password changing process. Opens the Change Password dialog box.

Menu Name	Submenu Name		Description
	Preferences		Opens the Preferences dialog box.
	Go Operational		Changes the AuC Server mode to operational.
	Go Out of Service		Changes the AuC Server mode to out off service.
Nationwide	Become Master		Initiates the process of becoming the Nationwide Master AuC, opens the AuC Connection dialog box, see AuC Connection on page 59.
	Become Slave		Initiates the process of becoming the Nationwide Slave AuC, opens the AuC Connection dialog box, see AuC Connection on page 59.
Help	AuC	Help Contents	Opens the AuC Online Help Contents.
		Introduction	Opens the Introduction section of the AuC Online Help.
		Overview	Opens the Overview section of the AuC Online Help.
		FAQ	Opens the FAQ section of the AuC Online Help.
	PrC	Help Contents	Opens the PrC Help Contents.
	About		Opens the About Enhanced Authentication Centre window.

NOTE: All menu items from the **File**menu are visible only while using Enhanced AuC view. While using AuC or PrC only views only PrC/AuC related items are displayed.

Chapter 3

AuC Installation and Configuration

3.1 AuC Server Application Installation

For information on the installation of the AuC Server Application, see the *Standalone Authentication Centre (AuC) Server Restoration* manual.

3.2 User Account Control

The User Account Control (UAC) feature helps maintain systems and PCs secure from malicious attacks by requiring authorization from users before running specific tasks or applications.

When a user with administrative privileges needs to perform a task that requires the administrator access token, the UAC feature automatically prompts the user for approval.

IMPORTANT: If a **User Account Control** window prompting you to allow an application you launched to make changes to your device appears, you must select **Yes**.

3.3 GUI Applications Access Permissions

To run the Enhanced Authentication Centre Client Application or Database Standby Monitor GUI, appropriate permissions must be set for the user. See Windows Local Groups on page 155.

3.4 Installing the Enhanced Authentication Centre Client Application

Procedure:

1. On the `C:\` drive, create an `Install_Files` folder. If prompted for administrator credentials or a confirmation, type the administrator credentials or click **Yes**.
2. Insert the Authentication Centre installation USB media into the USB port.

   IMPORTANT: If you are using the HPE Gen10 Server, do **not** use the iLO USB port.
3. Right-click the `EAUC-<version>.iso` image file, and select **Open with** → **Windows Explorer**.

   The ISO image is mounted to a new drive letter, and the content of the mounted ISO image automatically opens in Windows Explorer.
4. Copy the contents of the previously mounted image to `C:\Install_Files`
5. Navigate to `C:\Install_Files` and run `AuCClient-setup.exe`
6. On the welcome screen, click **Next**.

7. Select a destination folder for the application and click **Next**.
8. In the **Select Components** window, select **Enhanced AuC client with JRE** and click **Next**.
9. Specify the name of the folder where the shortcuts are created and click **Next**.
10. If you want to create additional icons on the desktop and in the start menu, select the **Create a desktop icon** and **Create a start menu icon** check boxes, and click **Next**.
11. Click **Install**.
12. After the installation is complete, restart the Windows operating system.

3.5
Configuring AuC after Installation

Follow procedure below to perform initial configuration of the Active Authentication Centre (AUC01).

Procedure:

1. The AuC Server automatically starts as a Windows service. The server needs about two minutes to initialize.
2. In the **Search** field, type in `mstsc` and press **Ctrl** + **Shift** + **Enter** to run Remote Desktop Connection as administrator.
3. In the Computer field, type the computer name, for example: `auc01.ucs1` , and then click **Connect**.

   NOTE: You can also type the IP address instead of the computer name.
4. Log on to an account with the appropriate permissions.
5. In the **Search** field, enter `Enhanced AuC Client`
6. Log on to Enhanced AuC Client.

   IMPORTANT: When logging into the AuC client for the first time, the user name and password are `admin` and `changeme1` respectively. You must change the admin password to a more secure one as soon as possible. See Changing a User Account Password on page 78.

   NOTE: Until initialization is completed the AuC Client will report an error when an attempt is made to log in.
7. Create the initial user(s). See Online Help for instructions how to create new users.

   NOTE: Only users with user management permission can add users to the system and assign their initial passwords. It is a requirement that the first user created must have full permissions, including user management.
8. Restart the AuC Client and log in with the new user name just created. Change the new user password as prompted.
9. Load the Master Key, according to instructions in Online Help.
10. In the AuC Client, select **Go Operational** from the **System** menu. The AuC will establish connections to the UCS. At this time, the AuC will also synchronize itself with the UCS. All Mobiles, KVLs, Zone, Security Groups, and KVL-Zone assignments will be updated in the AuC. The audit trail and events log can be reviewed to verify that all records have been added to the AuC database. Each respective tab: **Devices**, **KVLs**, and **Mobiles** should display all records. The **Mobiles** tab **Search** button will have to be clicked to update its display.
11. Check if each KVL has an UKEK assigned to it. If not, assign an appropriate UKEK. See Online Help for instructions how to assign UKEK key to a KVL.
12. Provision each infrastructure entity with a Ki, for instructions see Online Help.

13. Perform necessary key updates, according to Online Help instructions.

3.6 Installing the External Modem Driver for KVL to AuC/PrC Communication

Perform this procedure if you want to use the AuC/PrC to KVL modem connection.

This procedure can be performed only by members of the Administrators group.

If you use the StarTech USB56KEMH2 modem, Windows automatically configures the connection. See: Configuring KVL Port Settings on page 75. The modem should be attached and detached in `out of service` or `disabled` server mode.

Procedure:

1. Stop the AuC/PrC services:
   a. As an Administrators group member, on the AuC/PrC desktop, right-click the **Config Assistant** icon and select **Run as administrator**.
   b. In the **Config Assistant** window, enter: `ca disable`
2. Open **Control Panel** .
3. In the **All Control Panel Items** window, select **Phone and Modem**.
4. If the **Location Information** window appears, enter the required information and click **OK**.
5. In the **Phone and Modem** window, select the **Modems** tab.
6. Click **Add**.
7. In the **Add Hardware Wizard** window, select the **Don't detect my modem; I will select it from a list** check box. Click **Next**.
8. Select **Have Disk**.
9. In the **Install From Disk** dialog box, select **Browse**.
10. Perform one of the following actions:
    - If you use the MT5656ZDX modem, navigate to `C:\Motorola\AuC\<version>\drivers\modem\MT5656ZDX\5656.INF`, and click **Open**.
    - If you use the old MT9234ZBA modem, navigate to `C:\Motorola\AuC\<version>\drivers\modem\MT9234ZBA\MultitechA.INF`, and click **Open**.
11. In the **Install From Disk** dialog box, click **OK**.
12. From the **Models** list, select one of the following:
    - If you use the MT5656ZDX modem, select **MultiTech Systems MT5656ZDX**. Click **Next**.
    - If you use the old MT9234ZBA modem, select **MultiTech MT9234ZBA**. Click **Next**.
13. Ensure that the **Selected ports** radio button is selected, and perform one of the following actions:
    - For AuC, select **COM1** and click **Next**.
    - For PrC, select **COM2** and click **Next**.

    The installation process starts, followed by the confirmation message.
14. Click **Finish**.
15. Start the AuC/PrC services:

a. As an Administrators group member, on the desktop, right-click the **Config Assistant** icon and select **Run as administrator**.

b. In the **Config Assistant** window, enter: `ca enable`

Postrequisites: Ensure that the KVL ports are correctly configured. See Configuring KVL Port Settings on page 75.

3.7 Configuring KVL Port Settings

Configure the KVL port settings in the AuC/PrC Client application to enable the AuC/PrC to KVL direct communication or serial modem communication.

Procedure:

1. From the **System** menu, select **Preferences**.
2. In the **Preferences** window, in the tree view on the left, select **Port Settings**.
3. Perform one of the following actions:

If...	Then...
You want to enable the AuC/PrC to KVL direct communication,	perform the following actions: a. Under **Port settings for Key Variable Loader connection**, configure the following settings: i. **Port:** • For AuC, use **COM1**. • For PrC, use **COM2**. ii. **Type:** • For AuC, select **AuC**. • For PrC, select **PrC**. iii. **Connection:** Select **Direct**. iv. **Bit Rate:** Leave the default value (**19,200**). Ensure that this value matches the value set on the KVL. b. Click **OK**.

If...	Then...
You want to enable the AuC/PrC to KVL serial modem communication,	perform the following actions: **a.** Under **Port settings for Key Variable Loader connection**, configure the following settings: **i.** **Port:** • For AuC, use **COM1**. • For PrC, use **COM2**. **ii.** **Type:** • For AuC, select **AuC**. • For PrC, select **PrC**. **iii.** **Connection:** Select **Modem**. **iv.** **Bit Rate:** Select **19,200**. **b.** Ensure that `ATM0S0=1` appears in the **Initialisation String** column. **c.** Click **OK**.

The settings are saved.

IMPORTANT: On the server rear panel, the COM1 port is labeled **AuC** and the COM2 port is labeled **PrC**. Use these ports accordingly when establishing the connection.

Chapter 4

AuC Basic Operation

4.1 First Steps

This section introduces you to a number of tasks related to starting to work with the AuC application. These will be especially useful if you are a new user of the application. The following topics provide information on relevant procedures and reference information.

4.1.1 Starting the Authentication Centre Client Application

If you have not yet launched the Authentication Centre (AuC) application, follow procedure below to launch the client application.

NOTE:
If one or more error messages are displayed during start-up, refer to What to Do if an Error Message Appears when Starting the Client? on page 175 for assistance.

When you log into the client for the very first time after installation you will have to use the following default values:

- User Name: `admin`
- Password: `changeme1`

After logging on using default values, you are prompted to change the password. You must add a new user to the database. To begin the normal operation of the AuC, this user must be given user management permissions. See Creating an Enhanced AuC User Account on page 81. You should then exit the application and log on again using the new user values.

Procedure:

1. In the **Search** field, enter `Enhanced AuC Client`
2. In the **Enhanced Authentication Centre - Login** dialog box, type in your user name, password and the IP address of the server you want to connect to.

   For a procedure for changing the password, see Changing a User Account Password on page 78.

4.1.2 Changing View

After logging into the Enhanced AuC application all AuC and PrC tabs are visible on the GUI.

In the **View** menu, you can select one of the following options:

- **AuC only** - tabs only assosiated with AuC are displayed
- **PrC only** - tabs only assosiated with PrC are displayed
- **Enhanced AuC** - tabs assosiated with AuC and PrC are displayed

4.1.3
Changing a User Account Password

Procedure:

1. From the **System** menu, select **Change Password**.

   NOTE: When logging in for the first time the **Change Password** dialog box appears automatically and change of password is obligatory.

2. Type in the old and new passwords.

   NOTE: User names and passwords must comply with the user name and password requirements set up in the current User Settings. See Configuring User Settings on page 141.

3. Click **OK**.

   The password is changed for the next login.

4.1.4
Verifying Authentication Centre Status

Whenever you log into the AuC client, you should verify that the Authentication Centre (AuC) server is operational. To do this, locate Status Bar on page 32 and verify that the AuC Server Status icon is green ( ).

4.1.5
Displaying Key and Entity Information

One of the most frequently visited tabs in the AuC client is the **Devices** tab, which shows information about the zone, sites and current key status. Follow the procedure below to check the status of the zone or site entity.

Procedure:

1. To view Zone or Site entity status, select the **Devices** tab.
2. To view a specific Zone or Base Transceiver System (BTS) site entity's status, expand (if necessary) the tree view by clicking the plus icons next to the zones, and select the entity you want to view.

   When you select an entity, the respective key status is displayed in the work pane to the right.

4.1.6
Logging off from the Authentication Centre Client Application

Follow this procedure to log off from the Authentication Centre client application.

Procedure:

1. From the **File** menu, select **Exit**.
2. Confirm by clicking the **Yes** button.

4.2 Getting Help

The Authentication Centre (AuC) client is equipped with a context-sensitive online help system, that provides comprehensive information about the client application and how to work with it. To view context-sensitive help, select **Help** from the menu that you are working in. To view the full help system, select **AuC** or **PrC** from the **Help** menu, and then select **Help Contents**.

This section covers the following topics:

- Using Context Sensitive Help on page 79
- Using Full Text Search on page 79

4.2.1 Using Context Sensitive Help

As you work within the AuC client, you can obtain information about procedures, windows, and dialog boxes by using the context-sensitive help available in the application. You can access this help in several ways.

Table 95: Using Context Sensitive Help

Element	Description
Windows	Most windows display a **Help** button. Click the button and a topic opens in the online help window that provides links to information on related procedures and window fields and buttons.
Dialog Boxes	Some dialog boxes display a **Help** button. Click the button and a topic opens in the online help window that explains how to perform the procedure related to the dialog box.
Menu Commands	The AuC menu bar provides some commands under the **Help** menu to quickly navigate to specific type of information.

NOTE: The full online help system can be accessed from within each topic by clicking the **Show** hyperlink at the top of each page.

4.2.2 Using Full Text Search

When you enter a word or phrase in the online helps search field and press **Enter** key, the help system searches the contents of your topics to find all occurrences of that word or phrase. Its a good way to find a topic title (if you know it) or every instance of a concept or feature in the system.

4.3 Changing Authentication Centre Operating State

Procedure:

1. Locate the AuC Server Status icon in the status bar and note the current AuC server operating mode.

   NOTE: See Status Bar on page 32 for a listing and description of AuC server operating states.

2. To change the operating mode, perform one of the following:
   - To set the operating mode to Out of Service, from the **System** menu, select **Go Out of Service**.

- To set the operating mode to Operational, from the **System** menu, select **Go Operational**.

NOTE: See Table 2: Enhanced Authentication Centre (EAuC) States of Operation on page 33 for more information about AuC Server status values.

4.4 Viewing Enhanced Authentication Centre Version Information

In order to view EAuC version information click **Help** and then select **About** menu item. The **About Enhanced Authentication Centre** window appears showing you the Server Build, Client Build and Database Build numbers.

4.5 Generating Key Reports

There is a possibility to generate a report with keys currency for particular Zones/Sites and a general key currency used across the system. Follow the procedure below to generate key report.

Procedure:

1. From the application main menu, select **System** → **Key Report**.
2. Select a file name and press **Save** button.

   NOTE: Zone keys option allows to choose keys used for particular zone, site to be displayed in report. **AuC keys** option allows to choose keys used in the whole system.

   A **Key Report Contents** dialog box appears.
3. In the **Key Report Contents** dialog box, select what the generated key report has to include and click **OK**.
4. Click **OK**.

   The report is generated.

4.6 Users

The **Users** tab in the Authentication Centre (AuC) allows you to create, modify, and delete AuC client user accounts.

The following topics provide procedures associated with the **Users** tab in the AuC client display:

- Creating an Enhanced AuC User Account on page 81
- Modifying an Existing User Account on page 81
- Deleting an AuC User Account on page 81

The following topics provide reference information associated with the **Users** tab in the AuC client display:

- User Account Selection Tree View on page 55
- User Information on page 55
- Add User Dialog Box on page 58

4.6.1
Creating an Enhanced AuC User Account

Procedure:

1. From the **Users** tab, click the **Add** button.
2. Type in the user profile information.

   NOTE: The **Login Name** field allows spaces and is case-sensitive.
3. Select the appropriate check boxes to set the user security permissions and click **OK**.

   The user is stored in the AuC database, and now shows up in the user list on the left.

4.6.2
Modifying an Existing User Account

Procedure:

1. In the **Users** tab, select the appropriate user.
2. In the **User Information** pane, perform one of the following actions:

If...	Then...
If you want to change the user security permissions,	select or clear the appropriate check boxes.
If you want to modify the user account password,	perform the following actions: a. Select the **Change Password** check box. b. In the **New Password** field, enter the new password. c. In the **Confirm Password** field, enter the same password.

   NOTE: You cannot change your own password from this dialog box (when logged in as yourself). To change your own password, see Changing a User Account Password on page 78
3. To save changes click the **Apply Settings** button.

4.6.3
Deleting an AuC User Account

Procedure:

1. In the **Users** tab, select the appropriate user.
2. Click the **Delete** button.
3. To confirm the deletion, click the **Yes** button.

   The user is removed from the AuC database.

4.7
Events

The **Events** pane allows you to monitor actions and performance of the Authentication Centre (AuC).

When the AuC client window is launched, the Events Log displays the latest 300 server events. By default, new events are displayed at the top of the list box as they are received.

Events are displayed in a less complex form than the audit trail data. However, some of the events are duplicated in the audit trail.

The following are exemplary events:

- `Synchronization with Zone Manager(1) started.`
- `Synchronization with Zone Manager(1) completed successfully.`
- `New user (user1) was created by admin.`
- `UCS connection restored.`

For reference information associated with the **Events** pane, see Events Information on page 41.

4.7.1
Sorting Authentication Centre Events

The Authentication Centre (AuC) client window displays events in a scrolling list box. To sort the list of events, choose from the following:

Procedure:

The Authentication Centre (AuC) client window displays events in a scrolling list box. To sort events, perform the following:

- To sort events by severity, in the **Events** pane, click the **Severity** header.
- To sort events by date, in the **Events** pane, click the **Date** header.
- To sort events by description, in the **Events** pane, click the **Description** header.

4.7.2
Removing Authentication Centre Events

The Authentication Centre (AuC) client window displays events in a scrolling list box. Occasionally, you may want to shrink the event listing by removing one or more events from the list. Follow procedure below to remove an event or multiple events from the AuC Events display.

Procedure:

Choose from the following:

If...	Then...
If you want to remove certain event(s),	perform the following actions: **a.** In the **Events** pane, select the appropriate event(s). **b.** Click the **Remove** button.
If you want to remove all events	perform the following actions: **a.** Click the **Remove All** button. **b.** To confirm the removal, click the **Yes** button.

4.8
Audits

The **Audits** tab allows you to monitor actions and performance of the Authentication Centre (AuC).

Data in the audit trail sometimes overlap with data displayed in the **Events** pane, but the audit trail is more detailed and is targeted for advanced users.

Storage of the audit trail data can grow rapidly, so it is necessary to remove old audit trail data from the database.

There are two ways of audit removals:

- If there are more than 3 million audit trails, the oldest records are deleted automatically. It prevents the database size from increasing too heavily.
- The audit trail can be purged manually to an archive (CSV file).
  To purge the audit trail, see Removing Audits Data from the Database on page 83.

The following topics provide reference information associated with the **Audits** tab in the AuC client display:

- Events Information on page 41
- Audit Trail Information Display on page 38

4.8.1
Viewing Event Audits

The audit trail log stores a wide range of actions performed by the AuC. For example, the audit trail log maintains a record of all key management operations and allows you to trace the usage of a key, as it is distributed throughout the system. An audit of AuC operations can be viewed by specifying search criteria and viewing the query results in the AuC client window.

Procedure:

1. From the AuC Client window, open the **Audits** tab.
2. In the **Audit Search & Purge Form** pane, fill in the appropriate fields to meet your search criteria.
3. Click the **Search** button.
4. To hide the **Audit Search & Purge Form**, click on the **Hide Form** button.

   NOTE: To return to the previous **Audit Search & Purge Form** view, click the **Show Search Purge Form** button.

4.8.2
Removing Audits Data from the Database

Perform the following procedure to remove and archive the audit trail from the AuC database.

NOTE:
Purged audit trail is saved in a CSV format, in the following location:

<AUC_HOME>\var\audits\app

where *<AUC_HOME>* is the location where AuC is installed.

Prerequisites: Ensure that AuC user credentials used to perform this procedure have User Management security permissions.

Procedure:

1. From the AuC Client window, open the **Audits** tab.

2. Click the **Purge** button.
3. Using calendar buttons, select the date you want the purge to end.

   Audits after the selected date will **NOT** be purged.

   NOTE: Setting the date of a purge to 10-OCT-2018 means that purge is performed for all audits up to and including October 10, 2018.
4. Click the **Begin Purge** button, and click **OK**.

   The audits data is removed from the database and a new archived file is created.
   It is possible to open the archived CSV files using third party applications.

Chapter 5

Authentication and Air Interface Encryption Key Management

This chapter covers the following topics:

- Entity Status and Key Information on page 85
- Entering and Modifying Keys on page 94
- Key Distribution on page 106
- Enabling and Disabling Key Updates on page 117

5.1 Entity Status and Key Information

This section covers the following topics:

- Radio Key Information on page 85
- Viewing Radio Key Information on page 86
- Generating Radio Report on page 87
- Generating Mobiles OTAR Keys Report on page 87
- Viewing and Deleting Unmatched K-REF Pairs on page 88
- Generating an Unmatched K-Ref Pairs Report on page 90
- Zone Status and Key Information on page 91
- Viewing Zone Status and Key Information on page 91
- Site Status and Key Information on page 91
- Viewing Site Status and Key Information on page 92
- Viewing UCS Status on page 92
- ZDS Status on page 93
- Viewing KVL Key Information and Status on page 93

5.1.1 Radio Key Information

The AuC stores and manages authentication and air interface encryption keys used by subscriber radios that utilize the system infrastructure.

While not actually distributing to or updating keys in the radio, the AuC uses its knowledge of the radios authentication key (K) to create authentication material used by zone controllers to perform authentication. Using KS and KS keys (along with a random seed and random number), a radio can be authenticated by the system without transmission of the secret authentication key (K) stored in the radio at the factory.

The Authentication Centre (AuC) automatically retrieves and maintains records of all radios stored in the clusters User Configuration Server (UCS) which have a Radio ID assigned to them in the Reference Field. Each radio record is matched with an authentication key (K) loaded separately into the AuC via file import or manual entry.

For air interface encryption purposes, the AuC stores, distributes, and updates encryption keys used by the system. The AuC distributes the encryption keys to the zone and base site entities and regularly updates this key on a scheduled or on-demand basis.

The **Mobiles** tab in the Authentication Centre (AuC) provides information and tasks for performing key management of radios.

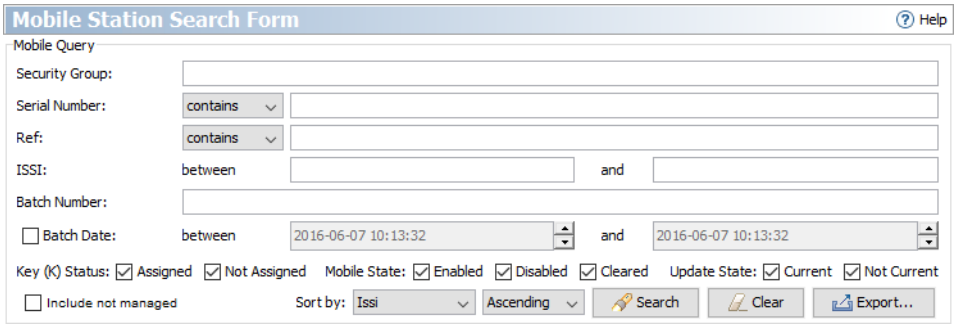
IMPORTANT: Any radio that does not have a REF assigned will not be stored or displayed by the AuC. These radios will not be provided with authentication material and therefore will be permitted to access the system without authentication.

5.1.2 Viewing Radio Key Information

Procedure:

1. Select the **Mobiles** tab.
2. In the **Mobiles** tab, **Mobile Station Search Form** pane, define the appropriate search criteria (search text is case-insensitive).

   Figure 17: The Mobile Station Search Form - Example



   NOTE: Specify the appropriate security group in order to execute a radio search. You can select a security group from the **Security Groups** tree display and the entry is automatically populated in the **Security Group** field.

   - The UCS Security Group functions as a “wildcard” in a search
   - Any fields that are left empty will not be included in the search

3. Click **Search**.

   The search results appear in the list window.

4. Locate the appropriate radio in the list window for current key information. The radios key information appears in the appropriate row in the list window.
5. In the list window double–click a row with desired mobile to display its Otar State window.

   IMPORTANT: To display Otar State window for a particular mobile it must be assigned to Crypto Management Group (CMG) and have enabled OTAR GSKO.

   The Otar State window appears.

5.1.3

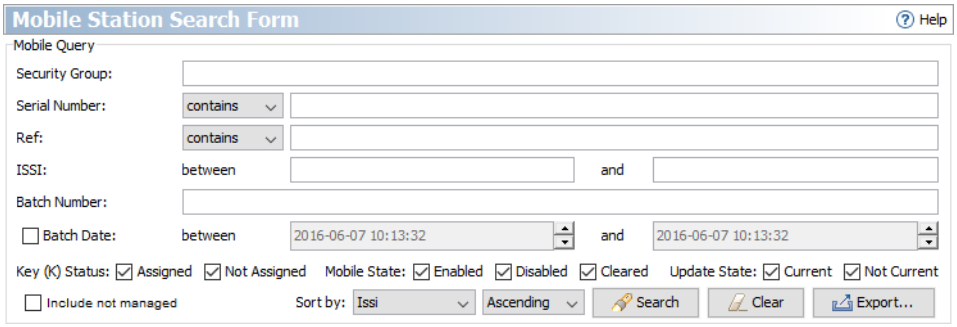
Generating Radio Report

The Authentication Centre allows a user to export information about all radios to a CSV or XML format file.

Procedure:

1. Select the **Mobiles** tab.
2. In the **Mobiles** tab, **Mobile Station Search Form** pane, click **Export** .

   Figure 18: Mobile Station Search Form



   A dialog box to select the export type appears.

3. Select the export type you want to save and click **OK**.

   A dialog box to select a location and format for the report file appears.

4. Select location and file format and click **Save**.

   A dialog box indicating the progress of the MS information export appears.

5. Click **OK**.

5.1.4

Generating Mobiles OTAR Keys Report

The Authentication Centre allows a user to run reports about current and not current mobiles and export the result to a CSV format file.

Procedure:

1. Select the **Mobiles** tab.

   The **Mobiles** tabbed pane appears.

2. Click the **Otar Report** button.
3. In the **Mobiles OTAR Keys Report** window, **Report Configuration** pane, **Report Type** group, select the **Not Current mobiles** or **Current mobiles** option.
4. From the **Available active CMGs** list select the applicable CMGs and click the **DOWN ARROW** button below the **Available active CMGs** list.

   NOTE: To move a CMG from the Selected CMGs list, select it and press the **UP ARROW** button.

   The CMGs selected appear in the **Selected CMGs** list.

5. Select the Key Type(s) to report.

   NOTE:

   - Mobile is listed as **Not Current** if at least one of the selected **Key Types** is not current for this mobile.
   - Mobile is listed as **Current** if all selected **Key Types** are current for this mobile.

6. Click the **Run report** button.

   When ready, the report appears in the **Result Summary** pane.

7. In the **Result Summary** pane, the **Mobiles tree** tab, click the **Export Report Summary** button.
8. In the **Save** window, select the location and ile name of the report. Click **Save**.

   NOTE: If a file with this name already exists, a confirmation dialog box appears.

9. A progress bar displays and closes when the generation of the report is complete and the dialog box stating that the report has been completed.

5.1.5
Viewing and Deleting Unmatched K-REF Pairs

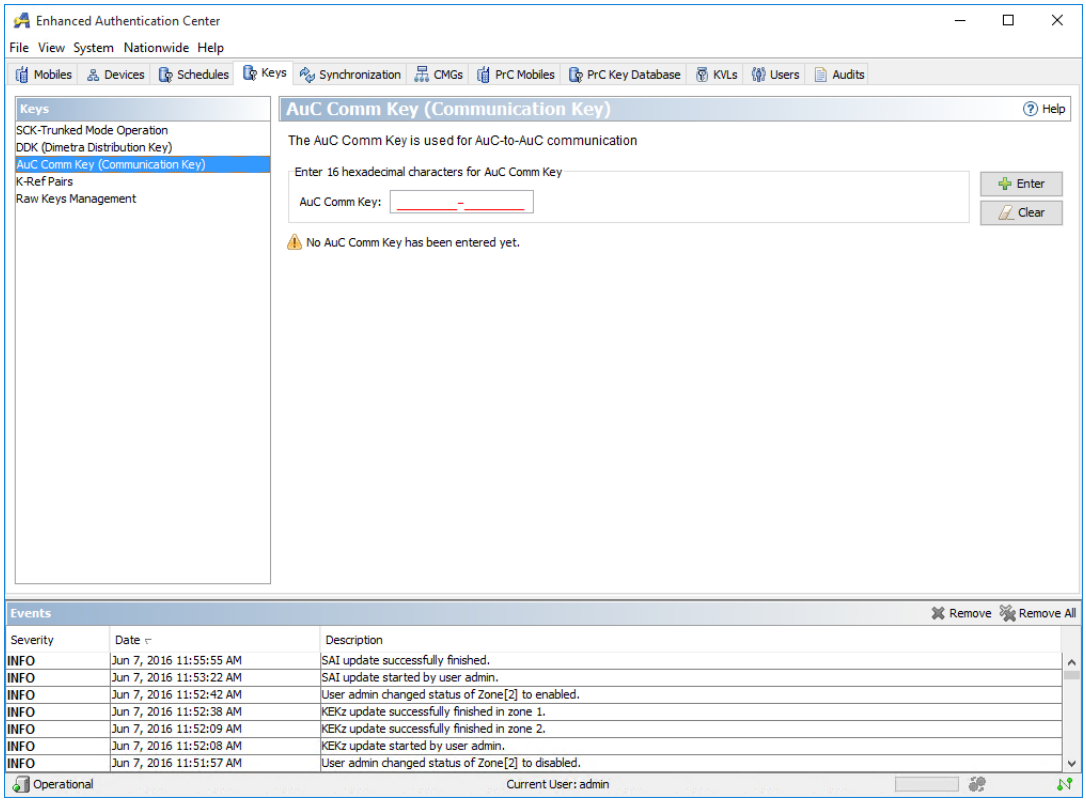
The AuC requires K-REF pairs to be loaded in to enable management of authentication keys (K) for radios. A K-REF pair is matched with an ITSI-REF pair (downloaded from the UCS) to correlate a radios ID and authentication key (K). When a K-REF pair cannot be matched with ITSI-REF pair, the K-REF pair is tagged as “unmatched” by the AuC.

WARNING: Unmatched K-REF pairs pose a security risk. If the unmatched K-REF pairs are redundant, you should delete them. You should also ensure that the deleted K-REF association is also removed from other Authentication Centres in the network, in cases where the K-REF pairs are duplicated across the network.

Procedure:

1. From the AuC client main window, select the **Keys** tab.

Figure 19: The Keys Tabbed Pane Example


Enhanced Authentication Center
File View System Nationwide Help
Mobiles Devices Schedules Keys Synchronization CMGs PrC Mobiles PrC Key Database KVLs Users Audits
Keys
SCK-Trunked Mode Operation
DDK (Dimetra Distribution Key)
AuC Comm Key (Communication Key)
K-Ref Pairs
Raw Keys Management
AuC Comm Key (Communication Key)
Help
The AuC Comm Key is used for AuC-to-AuC communication
Enter 16 hexadecimal characters for AuC Comm Key
AuC Comm Key:
Enter
Clear
No AuC Comm Key has been entered yet.
Events
Remove Remove All
Severity Date Description
INFO Jun 7, 2016 11:55:55 AM SAI update successfully finished.
INFO Jun 7, 2016 11:53:22 AM SAI update started by user admin.
INFO Jun 7, 2016 11:52:42 AM User admin changed status of Zone[2] to enabled.
INFO Jun 7, 2016 11:52:38 AM KEKz update successfully finished in zone 1.
INFO Jun 7, 2016 11:52:09 AM KEKz update successfully finished in zone 2.
INFO Jun 7, 2016 11:52:08 AM KEKz update started by user admin.
INFO Jun 7, 2016 11:51:57 AM User admin changed status of Zone[2] to disabled.
Operational
Current User: admin

The **Keys** tabbed pane appears.

2. Select **K-REF Pairs** in the **Keys** selection display.

   The K-REF pair information display appears in the work pane.

3. To display the list of unmatched K-Ref pairs, click the **Search** button.

   NOTE: You can narrow the search criteria and sort the search results.

   - To narrow the search criteria enter the Batch Number or Ref in an appropriate field. You can type in the whole number or just a part of it and than click **Search**.
   - To sort the unmatched K-Ref pairs select appropriate option from the list and click **Search**.

   The list of unmatched K-REF pairs is provided in the**Unmatched K-Refs** scrolling list box.

4. To delete a single K-REF pair from the AuC database, select the K-REF pair you want to delete from the list box.

   The selected K-REF pair is highlighted.

5. Click **Delete**.

   The **Delete Unmatched K-REF Pair** dialog box appears.

6. Click **Yes**.

   The K-REF pair is removed from the list box.

7. To delete all the unmatched K-REF pairs from the AuC database, click the **Delete All** button.
   The **Delete All Unmatched K-REF Pairs** dialog box appears.
8. Click **Yes**.

   NOTE: Depending on the amount of K-REF pairs, this can take long time.

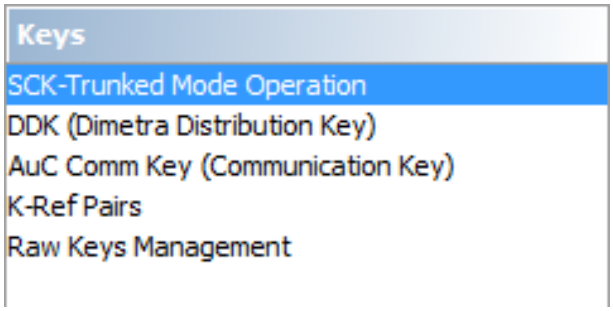
   The K-REF pairs are removed from the list box (the list box is empty).

5.1.6
Generating an Unmatched K-Ref Pairs Report

Procedure:

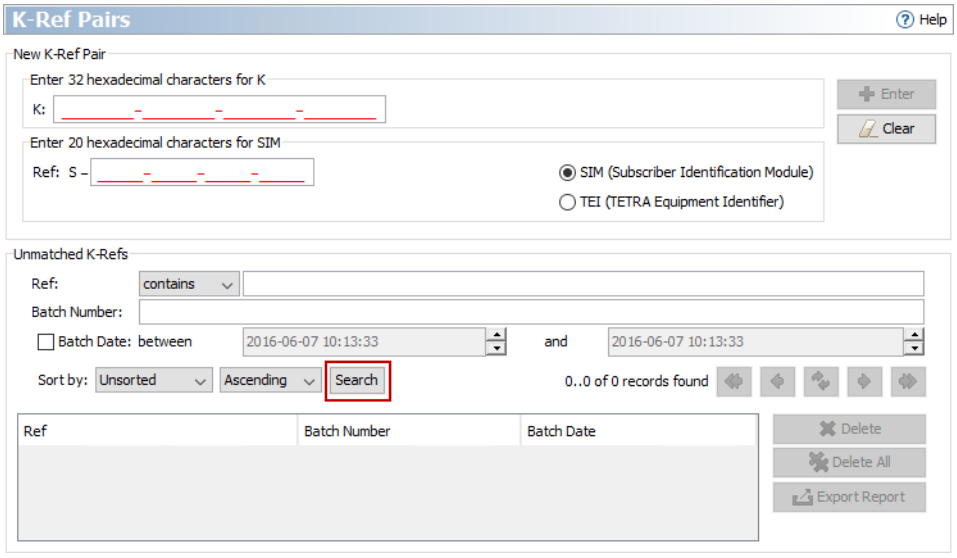
1. From the AuC client main window, select the **Keys** tab.
2. In the **Keys** tab, **Keys** pane, select **K-REF Pairs**.

   Figure 20: Keys Pane



3. To display the list of unmatched K-Ref pairs, in the **K-Ref Pairs** pane, click the **Search** button.

   Figure 21: K-Ref Pairs Pane



   The list of unmatched K-REF pairs is provided in the**Unmatched K-Refs** scrolling list box.

4. To generate a report of unmatched K-Ref pairs, click **Export Report**.
   A dialog box appears to choose a location of the generated report.

5. Select the location and file name of the report and click **Save**.

   NOTE: If a file with this name already exists, a confiration dialog box appears.

5.1.7
Zone Status and Key Information

The AuC stores and manages authentication and air interface encryption keys used by devices within the system infrastructure. To facilitate secure distribution and updating of keys through the system infrastructure, the AuC first generates an infrastructure key (Ki) for each zone and site entity.The Ki key is delivered from the AuC to each entity using the key variable loader (KVL) device. For zone entities, a system key encryption key (KEKm) and zone key encryption key (KEKz) are then delivered in encrypted form (using the Ki key) over the system infrastructure network to the entities.

The system zone controllers perform authentication of subscriber radios using authentication material generated and distributed by the AuC. The AuC distributes the proper KS and KS keys (along with a random seed and random number) in encrypted form (using the KEKm key) to the zone controllers on the system. The KS and KS keys are regularly updated on a scheduled or on-demand basis.

The current status of keys distributed to and stored in zone/site entities are tracked by the AuC. You can quickly observe the key status for a zone/site by locating its respective key status icon. You can also observe UCS connection status and version by locating its icon.

The **Devices** tab in the Authentication Centre (AuC) provides information and tasks for performing key management of zone infrastructure entities. The following topics provide procedures applying to zones entities and associated with the **Devices** tab in the AuC client display:

- Displaying Key and Entity Information on page 78
- Viewing Zone Status and Key Information on page 91
- Enabling/Disabling Key Updates for a Zone on page 119

The following topics provide reference information associated with the **Devices** tab in the AuC client display:

- Key Status Tree View on page 46
- Zone Information on page 57

5.1.8
Viewing Zone Status and Key Information

Procedure:

1. From the AuC client main window, select the **Devices** tab.
2. In the **Devices** tab, **Zones** pane, inspect the status of the zones.

   The zone icons are red, yellow or green according to the state the entitys keys are in. You can quickly observe a zones key status by locating its respective key status icon, see Table 29: Key Status Icons (Zones and sites) on page 47). To view all details about an entity keys, click the appropriate icon in the **Zones** pane.

   The zones key information appears in **Zone Detailed View** pane.

5.1.9
Site Status and Key Information

The AuC stores and manages authentication and air interface encryption keys used by devices within the system infrastructure. To facilitate secure distribution and updating of keys through the system

infrastructure, the AuC first generates an infrastructure key (Ki) for each zone and site entity.The Ki key is delivered from the AuC to each entity using the key variable loader (KVL) device. For site entities, a zone key encryption key (KEKz) is delivered in encrypted form (using the Ki key) over the system infrastructure network to the entities.

For air interface encryption purposes, the AuC stores, distributes, and updates the trunked mode static cipher keys (TM-SCK), the common cipher keys (CCK), the modified group cipher keys (MGCK) and the direct mode static cipher keys (DM-SCK) used by the system. The AuC distributes these keys encrypted (with the KEKz key) to base sites and regularly updates the keys on a scheduled or on-demand basis.

The AuC automatically retrieves and maintains records of site entities stored in the zones Zone Database Server (ZDS). Each site entity record is assigned encryption keys generated or loaded into the AuC.

The **Devices** tab in the Authentication Centre (AuC) provides information and tasks for performing key management of site infrastructure entities. The following topics provide procedures applying to site entities and associated with the **Devices** tab in the AuC client display:

- Displaying Key and Entity Information on page 78
- Viewing Site Status and Key Information on page 92
- Enabling/Disabling Key Updates for a Site on page 119

The following topics provide reference information associated with the **Devices** tab in the AuC client display:

- Key Status Tree View on page 46
- BTS Site Information on page 40

5.1.10
Viewing Site Status and Key Information

Procedure:

1. From the AuC client main window, select the **Devices** tab.
2. In the **Devices** tab, **Zones** pane, inspect the status of the zones.

   The zone icons are red, yellow or green according to the state the entitys keys are in. You can quickly observe a zones key status by locating its respective key status icon, see Table 29: Key Status Icons (Zones and sites) on page 47). To view all details about an entity keys, click the appropriate icon in the **Zones** pane.

   The site key information appears in **Site Detailed View** pane.

5.1.11
Viewing UCS Status

The Authentication Centre (AuC) automatically retrieves and maintains records of zone and site entities stored in the systems User Configuration Server (UCS). Each zone/site entity record is assigned encryption keys generated or loaded into the AuC.

The **Synchronization** tab, allows you to synchronize with the UCS and ZDSes and check their current status. See also UCS Information on page 54 for additional information.

Procedure:

1. From the AuC client main window, select the **Synchronization** tab.
2. To view the UCS status, select the UCS entity in the **Servers** pane.

The UCS icon reflects the connection status.

The **User Configuration Server** pane appears.

5.1.12
ZDS Status

NOTE: For viewing ZDS status perform Viewing UCS Status on page 92 choosing ZDS instead of UCS entity while executing step 2.

5.1.13
Viewing KVL Key Information and Status

Each KVL is assigned specific zone and site entities to update by the system. Using the KVLs unique key encryption key (UKEK) key, the AuC transfers the appropriate Ki keys to the KVL during a AuC/KVL communications session. Once transferred to the proper entities, the KVL re-initiates a communications session with the AuC and transfers download acknowledgments (received from the entities) to the AuC.

The AuC automatically retrieves and maintains records of key variable loader (KVL) entities stored in the systems User Configuration Server (UCS). Each KVL entity record is assigned a UKEK key loaded separately into the AuC via manual entry.

The **KVLs** tab in the Authentication Centre (AuC) provides key management information for the external key variable loaders (KVLs) used by the AuC.

The **KVLs** tab in the Authentication Centre (AuC) provides key management information for the external key variable loaders (KVLs) used by the AuC. The following topics provide procedures associated with the **KVLs** tab in the AuC client display:

- Entering a UKEK Key for a KVL Device on page 105
- Enabling/Disabling KVL Access to the Authentication Centre on page 120

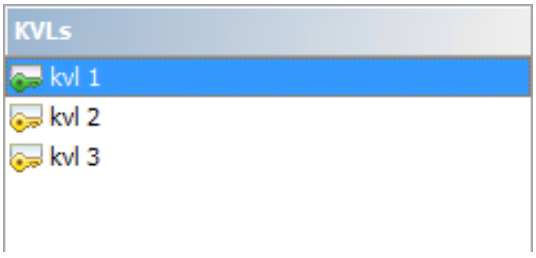
The following topics provide reference information associated with the **KVLs** tab in the AuC client display:

- KVL Information on page 47
- KVL Status List View on page 48
- Port Settings on page 65
- KVL UKEK Assignment Dialog Box on page 63

Procedure:

1. From the AuC client main window, select the **KVLs** tab.
2. In the **KVLs** tab, **KVLs** pane, select the appropriate KVL device in the **KVLs** list display.

   Figure 22: KVLs Pane Example



If...	Then...
The key status icon has a green color,	KVL is provisioned in the AuC database.

If...	Then...
The key status icon has a yellow color,	KVL is not provisioned in AuC database (due to no assigned UKEK key).
The key status icon has a red color,	KVL is locked out from connectivity to AuC (this is set within the AuC.

The KVLs current key status is reflected in both the icon color, and in the **KVL Information** pane.

5.2 Entering and Modifying Keys

The **Keys** tab in the Authentication Centre (AuC) provides the ability to load and store K-REF pairs for radios, trunked mode static cipher keys (TM-SCK), the authentication communication key (AuC Comm Key), the DIMETRA Distribution key (DDK) and raw keys.

5.2.1 Entering K-REF Pairs into the Authentication Centre

The AuC requires the loading of K-REF pairs to enable management of authentication keys (K) for radios. A K-REF pair is matched with an ITSI-REF pair (downloaded from the UCS) to correlate a radios ID and authentication key (K).

K-REFs can be entered manually or they can be imported from another media, for example, a CD.

NOTE: This procedure allows you to type in the K-REF pair from the keyboard. To import a K-REF pair file, see Importing a K-REF Pair File into the Authentication Centre on page 96.

Follow the procedure below to enter K-REF pairs manually into the AuC.

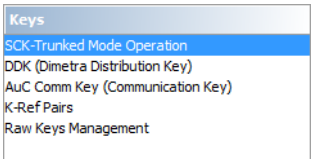
Procedure:

1. From the AuC client main window, select the **Keys** tab.

   The **Keys** tabbed pane appears.

2. In the **Keys** tab, **Keys** pane, select **K-REF Pairs**.

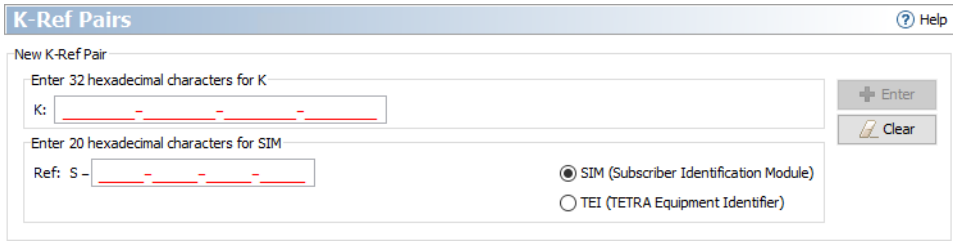
   Figure 23: Keys Pane

3. **NOTE:** K-REF pairs cannot be automatically generated by the AuC. They are generated by the Provisioning Centre (PrC), or created externally by, for example a secure authority. They can be entered manually using the AuC.

   - Type in the authentication key (K) for the MS in the **K** field
   - Using the radio buttons, select the REF type (SIM or TEI) used for the MS
   - Type in the REF for the MS in the **Ref** field

Figure 24: K-REF Pairs Pane



4. Click **Enter**.

   NOTE: The **Enter** button will remain grayed out until all of the required information has been entered in the appropriate fields.

   Confirmation message appears in the **Events** tab display. The batch date is set to the current time and the batch number is left blank. You can refresh the unmatched K-Refs list by clicking the refresh button.

5. Decide whether you want to overwrite existing K-Ref pair or not.

   NOTE: If the user enters a K-REF pair where the Ref part already exists in a K-REF pair in the AuC, a confirmation box appears.

5.2.2
Transfering K-REF Pairs into the Authentication Centre

This procedure is an alternative for exporting keys from the PrC, saving them on a carrier, and then importing them from a file to the AuC.

Procedure:

1. From the Enhanced AuC client main window, select the **PrC Mobiles** tab.
2. In the **Mobile Station Search Form** pane, search for the K-Ref pairs that you want to transfer. Enter appropriate search criteria in the form and click **Search**.
3. Click the **Transfer K-Refs** button.

   NOTE: If search returns 0 Mobiles, the button is greyed out.

   The **Transfer K-Refs** window appears. After the calculation of the number of KRef pairs to transfer is finished the number of KRef pairs to be transferred is displayed.

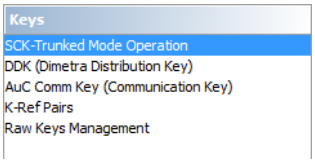
4. In the **Transfer K-Refs** window, click **Continue**.

   NOTE: If some of the KRef pairs already exist in the AuC database the Overwritten, Skipped and Custom options will be active. Custom option is active when the number of the KRefs existing already in the AuC database is less than, or equal, a thousand.

   When the transfer is complete, the results appear in the **Events** pane.

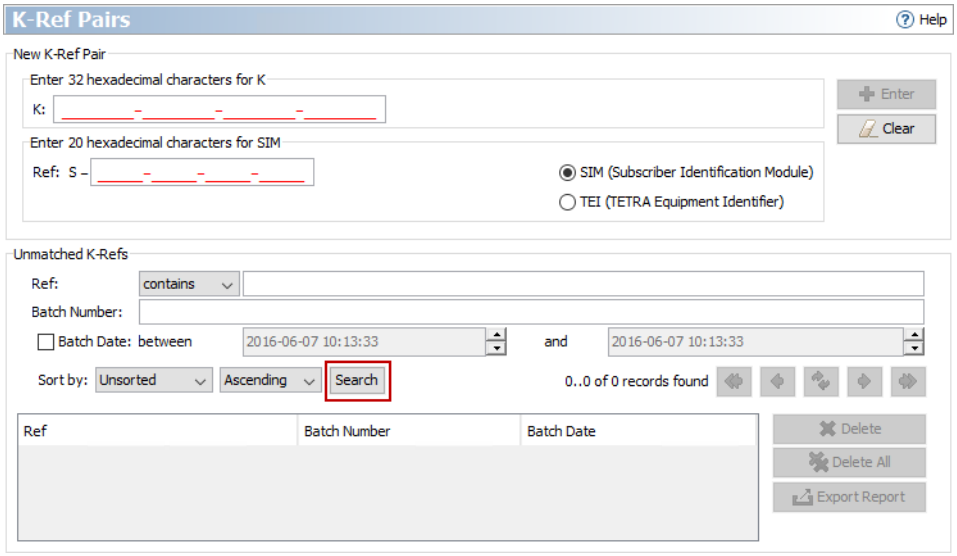
5. After transferring K-Refs, you can verify K-Ref keys in **Keys** tab:
   a. Select the **Keys** tab.
   b. In the **Keys** tab, **Keys** pane, select **K-Ref**

Figure 25: Keys Pane



c. In the **K-Ref Pairs** pane, **Keys** pane, click **Seach**.

Figure 26: Keys Pane Example



5.2.3
Importing a K-REF Pair File into the Authentication Centre

The AuC requires the loading of K-REF pairs to enable management of authentication keys (K) for radios. A K-REF pair is matched with an ITSI-REF pair (downloaded from the UCS) to correlate a radios ID and authentication key (K). The PrC is the source of the K-REF pairs.

NOTE: This procedure allows you to import a K-REF pair file. To manually type a K-REF pair into the AuC, see Entering K-REF Pairs into the Authentication Centre on page 94.

Procedure:

1. From the AuC client application main menu, select **File** → **Import to AuC** → **K-Ref Pairs**.
2. In the **Import From** window, navigate to the K-REF pair file that you want to import. Click **OK**.
3. Click **Import**.
4. If prompted, in the **Import Key Confirmation** window, select the desired setting and click **Continue**.

   Upon completion, information about imported K-Ref pairs appears in the **Events** pane.

5.2.4

Importing an SCK-TMO Key File into the Authentication Centre

A static cipher key-trunked mode operation (SCK-TMO) key file contains a list of 32 numbered SCK-TMO keys. Each key in the file is assigned a number and version and is handled as such by AuC.

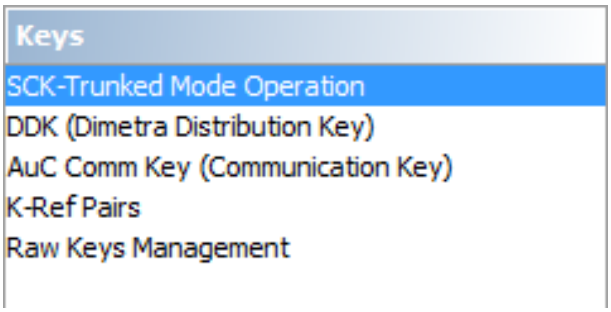
IMPORTANT: All SCK key slots should be populated in the AuC. If an empty key slot is selected as the **Next Active** key then the key update will not take place until the slot has been populated.

WARNING: If a new set of SCK-TMO keys is imported, the same keys must be provisioned to the MSs. If they are not, encryption using SCK-TMO will not be possible.

Procedure:

1. From the AuC client main window, select the **Keys** tab.
2. In the **Keys** tab, **Keys** pane, select **SCK-Trunked Mode Operation**.

   Figure 27: Keys Pane

   The **SCK-TMO** pane appears.
3. From the application main menu, select **File** → **Import** → **SCK Keys**.
4. In the **Import From** window, navigate to the SCK-TMO file that you want to import.
5. Click the **Import** button.

   NOTE: All SCK slots in the SCK-TMO file must be filled, otherwise import will be impossible.

   The AuC scans the selected file to determine content type. When completed, the following alert box appears.
6. Click **OK**.

   NOTE: Importing new SCKs will cause a partial distribution of keys, if the AuC is part of a Nationwide system, the keys will be distributed to the other AuCs.

   The keys are imported into the AuC database.

5.2.5

Modifying an SCK-TMO Key in the Authentication Centre

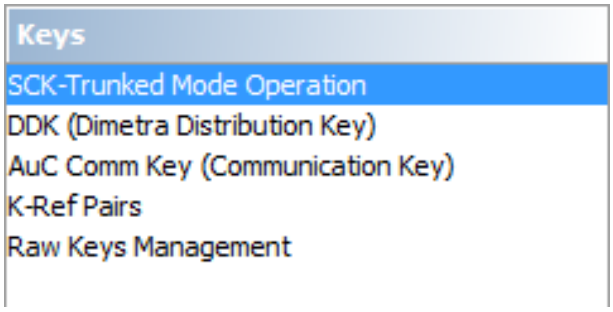
The AuC stores 32 numbered static cipher key-trunked mode operation (SCK-TMO) keys. You can modify the number or version of any SCK-TMO key using the AuC main client window.

WARNING: If an SCK-TMO key is modified after it has been provisioned to the MSs air interface encryption using this key will not be possible.

Procedure:

1. From the AuC client main window, select the **Keys** tab.
2. In the **Keys** tab, **Keys** pane, select **SCK-Trunked Mode Operation**.

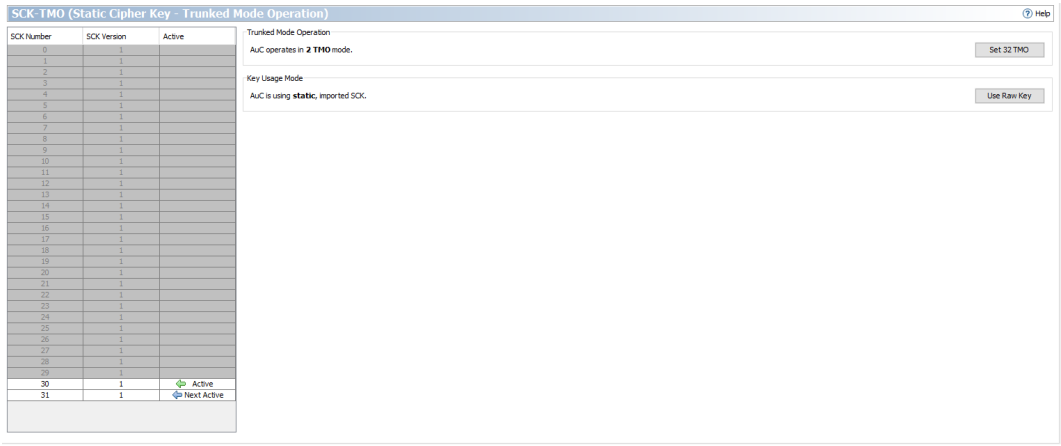
   Figure 28: Key Pane

   The **SCK-TMO** pane appears.

3. In the **SCK-TMO (Static Cipher Key - Trunked Mode Operation)** pane, select the key slot row to modify.

   Figure 29: SCK-TMO (Static Cipher Key - Trunked Mode Operation) Pane

4. Right-click the highlighted row and select **Modify**.
5. In the **Enter Static Cipher Key** window, **Key Value** field, enter the key.
6. Select the key version number in the **Key Version** field and click **OK**.

   NOTE: The **OK** button will remain grayed out until all of the required information has been entered in the appropriate fields.

   The key information is updated.

5.2.6

Setting the Next Active SCK-TMO Key

The Authentication Centre (AuC) server designates the active static cipher key-trunked mode operation (SCK-TMO) key to be used by the system. When an SCK-TMO key update occurs, the active key (signified by the Active arrow in the Active column) is moved to the slot designated by the Next Active arrow in the Active column. See the arrows icons below:

	Active arrow
	Next Active arrow

NOTE: Only one SCK-TMO can be active at a time.

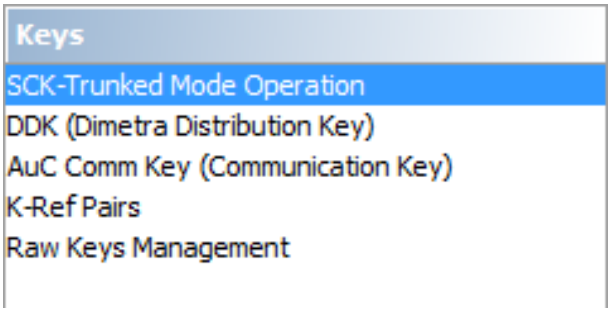
IMPORTANT: Performing this task enables changing the active SCK-TMO throughout the system during the next SCK-TMO key update. There is no resulting disruption to system operations by this task. When the key update occurs, the AuC communicates the change to each BTS site on the system. To determine if a BTS site is using the new active SCK-TMO key, see Viewing Site Status and Key Information on page 92.

Follow procedure below to set the next active SCK-TMO key in the AuC.

Procedure:

1. From the AuC client main window, select the **Keys** tab.
2. In the **Keys** tab, **Keys** pane, select **SCK-Trunked Mode Operation** .

   Figure 30: Keys Pane

   The **SCK-TMO (Static Cipher Key - Trunked Mode Operation)** pane appears.
3. In the **SCK-TMO (Static Cipher Key - Trunked Mode Operation)** pane, select the key slot row you want to set as a next active.
4. Right-click the selected row and select **Set Next Active**.
5. In the **Change Next Active SCK Number** confirmation box, click **Yes**.

   The Next Active slot is updated.

5.2.7

Changing Trunked Mode Operation

For DM-SCK OTAR to be enabled, 2 TMO mode is required.

NOTE:
Before switching between 32 TMO mode and 2 TMO mode, the following criteria **must** be met:

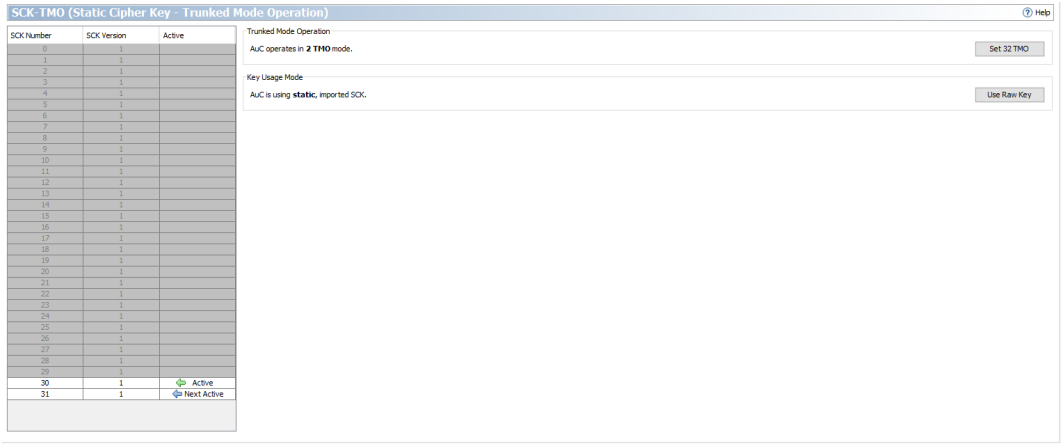
- **From 32 TMO to 2 TMO:** There must be active and inactive TM-SCK keys in slots TM-SCK number **30** and TM-SCK number **31**.
- **From 2 TMO to 32 TMO:** DM-SCK OTAR for all active CMGs must be disabled

WARNING: Switching back from 2 TMO to 32 TMO is highly discouraged after OTAR was enabled in the system, since subscribers may have already overwritten their SCK keys on numbers 0 to 29. This may lead to necessity of re-provisioning all subscribers and AuC with SCK keys map, if TM-SCK OTAR is not enabled for all subscribers.

Procedure:

1. From the AuC client main window, select the **Keys** tab.
2. In the **Keys** tab, select **SCK-Trunked Mode Operation** in the **Keys** selection display.

   Figure 31: SCK-Trunked Mode Operation Display - Example



   The **SCK-TMO** information display appears in the work pane.

3. Perform one of the following:
   - To switch from 32 TMO mode to 2 TMO mode, click the **Set 2 TMO** button.
   - To switch from 2 TMO mode to 32 TMO mode, click the **Set 32 TMO** button.

   NOTE: If the Set 2 TMO button is inactive, switching is not allowed. If so, make sure the above stated criteria are met.

5.2.8

Changing Key Usage Mode

NOTE:
Before switching from Static Key mode to Raw Key mode, please note the following:

- Changing from Static Key mode to Raw Key mode means that each TM-SCK update will cause a change of key material and key version in the TM-SCK map. Consequently, a new key will be used in the system and all subscribers will have to acquire that key by OTAR.
- Changing from Raw Key mode to Static Key mode means that each TM-SCK update will use the same key material as currently being used in the TM-SCK map on the AuC.

NOTE:
Before switching between Static mode and Raw mode, the following criteria **must** be met:

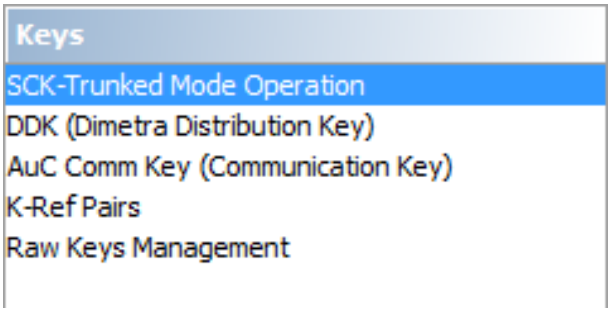
- **Static to Raw:** Each subscriber in the system has to be in ISSI range of some CMG, that has TM-SCK OTAR enabled. This means all subscribers should be able to receive TM-SCK OTAR updates via air interface.

WARNING: After this transition TM-SCK OTAR has to remain enabled for all subscribers, even after going back to Static mode. All new subscribers in the system should be SCK OTAR ready and within a range of TM-SCK OTAR enabled CMG, because they cannot be provisioned with SCK map anymore.

Procedure:

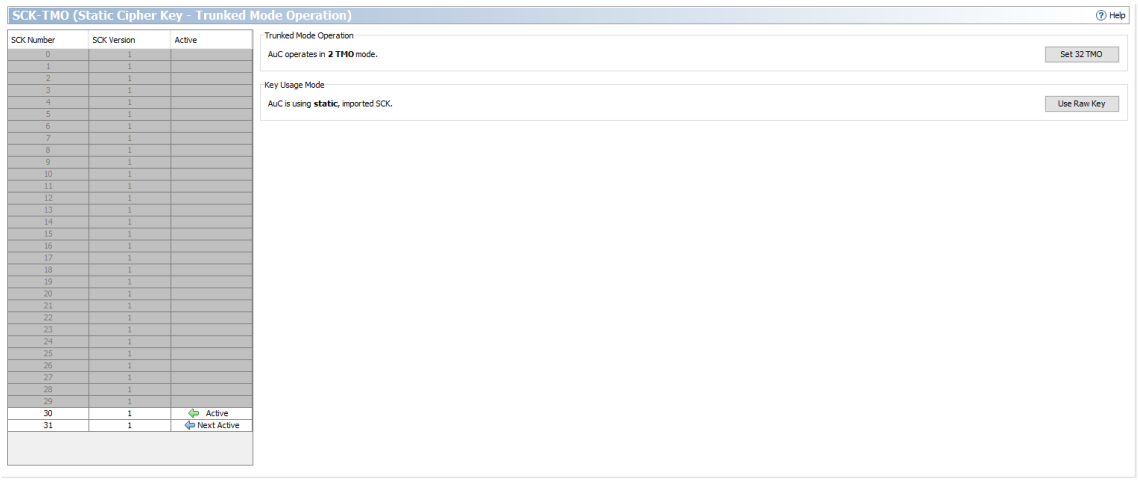
1. From the AuC client main window, select the **Keys** tab.

   Figure 32: Keys Tabbed Pane

2. In the **Keys** tab, **Keys** pane, select **SCK-Trunked Mode Operation**.

Figure 33: SCK-Trunked Mode Operation Display - Example



The **SCK-TMO** information display appears in the work pane.

3.
   - Switching to Raw Key mode is performed by clicking the **Use Raw Key** button.
   - Switching to Static Key mode is performed by clicking the **Use Static Key** button.

5.2.9
Entering the AuC Communications Key

The AuC Communication Key (AuC CommKey) is used by all nationwide AuCs to transport key information securely between AuCs.

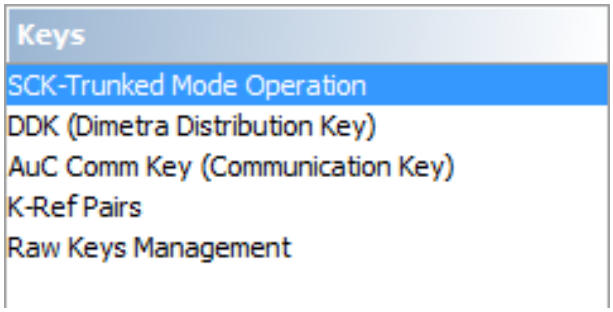
IMPORTANT: Since all AuCs need the same AuC CommKey, a synchronized key change is recommended to ensure proper system communication. It is also recommended to temporarily disable key schedules while an AuC CommKey change takes place.

Follow procedure below to define the AuC Communications Key.

Procedure:

1. From the AuC client main window, select the **Keys** tab.
2. In the **Keys** tab, **Keys** pane, select **AuC Comm Key (Communication Key)**.

   Figure 34: Keys Pane

   The **AuC Comm Key** pane appears.

3. In the **AuC Comm Key** pane, enter the key information into the **AuC CommKey** field.

4. Click the **Enter** button.

   NOTE: The **Enter** button will remain grayed out until all of the required information has been entered in the appropriate fields.

   The **Status** field display is updated.

5.2.10 Entering a DIMETRA Distribution Key

The DIMETRA Distribution Key (DDK) was utilized in DIMETRA system releases prior to release 5.0. This key must be entered in the Authentication Centre (AuC) to facilitate replacement of the DDK key with the infrastructure key (Ki) in Base Transceiver Bases System (BTS) site entities.

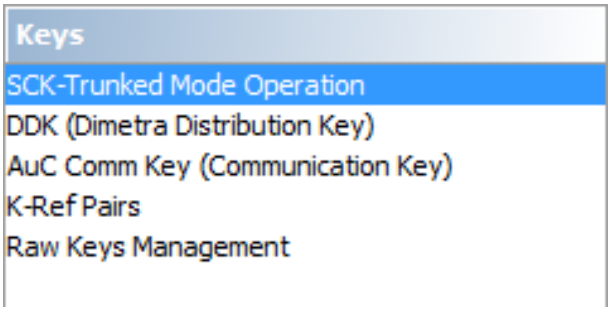
IMPORTANT: This task is necessary only when upgrading from a DIMETRA Release 4.x system, or earlier.

Follow procedure below to enter an existing DDK key into the AuC database.

Procedure:

1. From the AuC client main window, select the **Keys** tab.
2. In the **Keys** tab, **Keys** pane, select **DDK (Dimetra Distribution Key)**.

   Figure 35: Keys Pane



3. In the **DDK** pane, enter the DDK key.
4. Click **Enter** button.

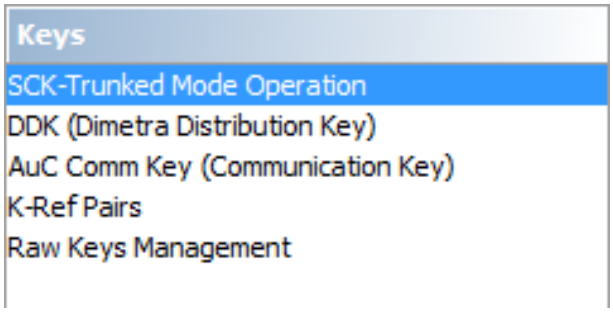
   The **Status** field in the **DDK (Dimetra Distribution Key)** information display is updated.

5.2.11 Generating Raw Keys Automatically

Procedure:

1. From the AuC client main window, select the **Keys** tab.
2. In the **Keys** tab, **Keys** pane, select **Raw Keys Management**.

Figure 36: Keys Pane



The **Raw Keys Management** pane appears.

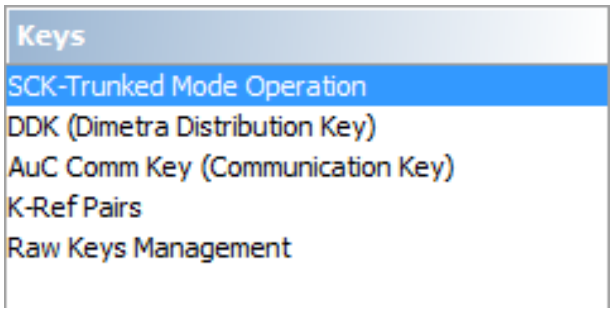
3. In the **Raw Keys Management** pane, select **Generated by encryption device** option for all keys types and click **Apply**.

5.2.12 Retrieving Raw Keys from the Imported File

Procedure:

1. From the AuC client main window, select the **Keys** tab.
2. In the **Keys** tab, **Keys** pane, select **Raw Keys Management**.

   Figure 37: Keys Pane



   The **Raw Keys Management** pane.

3. In the **Raw Keys Management** pane, select the **Retrieved from the pool of imported keys** option and adjust the **Pool Threshold**.

   IMPORTANT: If there are less keys in the pool in the database than it is set up in the **Pool Threshold** field the warning message will appear.

   NOTE: You can delete all the keys from the pool by clicking **Delete All**

4. Click **Apply**.

5.2.13
Importing Raw Keys from a File

Procedure:

1. From the AuC client main window, select **File** → **Import** → **Raw Keys** from the main menu.
   The following window appears.
2. Select the file you want to import the keys from and click **Open**.
   Progress window is displayed.
3. Click **OK** to finish importing the keys.

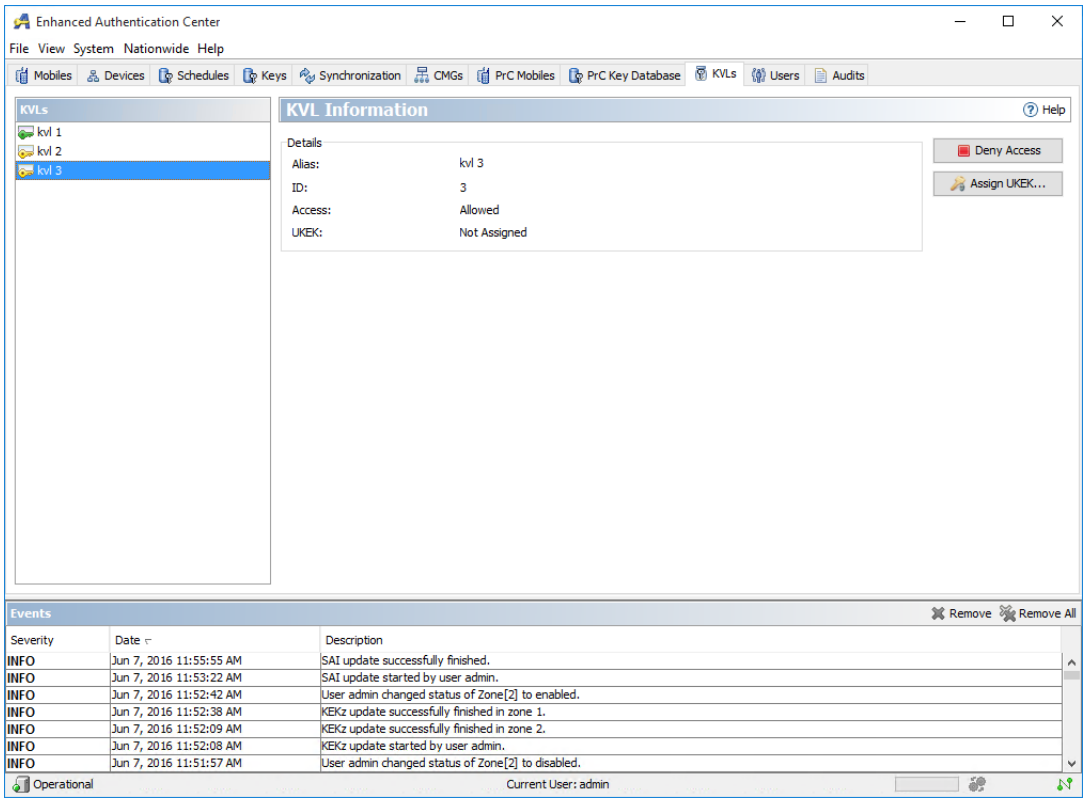
5.2.14
Entering a UKEK Key for a KVL Device

When receiving a key variable loader (KVL) entity record from the User Configuration Server (UCS), the AuC indicates on the **KVLs** tab that it is necessary to enter a Unique Key Encryption Key (UKEK) key for the KVL.

NOTE: The same UKEK key needs to be entered into the KVL.

Procedure:

1. From the AuC client main window, select the **KVLs** tab.
   Figure 38: KVLs Tabbed Pane Example


Enhanced Authentication Center
File View System Nationwide Help
Mobiles Devices Schedules Keys Synchronization CMGs PrC Mobiles PrC Key Database KVLs Users Audits
KVLs
kvl 1
kvl 2
kvl 3
KVL Information
Help
Details
Alias: kvl 3
ID: 3
Access: Allowed
UKEK: Not Assigned
Deny Access
Assign UKEK...
Events
Remove Remove All
Severity Date Description
INFO Jun 7, 2016 11:55:55 AM SAI update successfully finished.
INFO Jun 7, 2016 11:53:22 AM SAI update started by user admin.
INFO Jun 7, 2016 11:52:42 AM User admin changed status of Zone[2] to enabled.
INFO Jun 7, 2016 11:52:38 AM KEKz update successfully finished in zone 1.
INFO Jun 7, 2016 11:52:09 AM KEKz update successfully finished in zone 2.
INFO Jun 7, 2016 11:52:08 AM KEKz update started by user admin.
INFO Jun 7, 2016 11:51:57 AM User admin changed status of Zone[2] to disabled.
Operational
Current User: admin

2. In the **KVLs** tab, **KVLs** pane, locate and select the appropriate KVL.
   The KVLs key information appears in the work pane.

3. To assign a new UKEK key for the selected KVL, click the **Assign UKEK** button.
4. In the **Assign UKEK** window, enter the UKEK key in the field.

   NOTE: The UKEK entered must match the one stored in the KVL.
5. Click **OK**.

   The key assignment is confirmed in the **Events** display.

5.3 Key Distribution

This section provides procedures for distributing infrastructure keys (Ki) to zone and site entities. This section provides also procedures for performing key updates to DIMETRA system entities.

IMPORTANT:
The following parameters must be set correctly in the UCS:

- Security Class Change Notification Period = 5 seconds.
- Key Change Notification Period = 300 seconds.
- Security Class Hysteresis Period = 300 seconds.

NOTE: The BTS will wait a **minimum** time equivalent to the settings of SCCNP, SCHP and KCNP.

IMPORTANT:
If at least one Ki acknowledgment message is received by AuC from an entity (Zone or site), then the entity is no longer listed in the KVL. Thus, before reconnecting the KVL to the AuC server, make sure that the Ki is provisioned to all entities that require the Ki, that is:

- when provisioning Zones:
  - primary and standby Zone Controllers (ZC)
- when provisioning sites:
  - primary and standby TETRA Site Controllers (TSC)
  - complete set of Base Radios (BR)

If you need the entity to be listed in the KVL again, use the **Refresh Ki** or **Update Ki** button for this entity in the AuC client and then connect the KVL to the AuC server.

5.3.1 Logging On to the Server

Using an appropriate IP address and a PuTTY client, you can log on to a server or Improved Generic Application Server (iGAS) to re-install, configure, or restart a server.

Prerequisites: Power on the server.

Procedure:

1. Start PuTTY.
2. Optional: In the **PuTTY Configuration** window, in the **Category** navigation pane, expand the **SSH** node and select **Kex**.
3. Optional: In the **Options controlling SSH key exchange** pane, from the **Algorithm selection policy** list, select **Diffie-Hellman group 14** and click **Up**, until **Diffie-Hellman group 14** appears on the top of the list.

4. In the **Category** navigation pane, click **Session**.
5. In the **Basic options for your PuTTY session** pane, in the **Host Name (or IP address)** field, enter the IP address of the server. See your DIMETRA IP Plan.

   At the first attempt to log on, the **PuTTY Security Alert** window appears. For details on messages appearing when establishing the SSH session, see Messages Appearing when Establishing a Secure Session on page 107.
6. Start the session by clicking **Open**.
7. In the **PuTTY Security Alert** window, perform one of the actions:
   - To add the server rsa2 key to the PuTTY cache and connect, click **Yes**.
   - To connect without adding the server rsa2 key to the PuTTY cache, click **No**.
8. At the logon prompt, enter the user logon name.
9. At the password prompt, enter the current password.

5.3.1.1

Messages Appearing when Establishing a Secure Session

When establishing a secure session with iGAS or an application server, messages appear indicating different server states and possible risks.

Thie following table contains example messages likely to appear when logging on to a server.

NOTE: The IP addresses and RSA key fingerprints are unique per server and vary depending on the system configuration.

Table 96: Messages Appearing when Establishing a Secure Session

Message Example	Explanation
`The authenticity of host '<XXX.XX.XXX.X> (<XXX.XXX.XXX.XXX>)' can't be established. RSA key fingerprint is <yyy:yyy:yyy:yyy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy>. Are you sure you want to continue connecting (yes/no)?` where *<XXX.XXXX.XXX.XXX>* is the IP address of the host and *<yyy:yyy:yyy:yyy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy>* are RSA key fingerprints of the server.	This message, or a similar message depending on the SSH client used, is normal and expected to appear at the first attempt to log on to a server.
`The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is. The server's rsa2 key fingerprint is: ssh-rsa <yyy:yyy:yyy:yyy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy> If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting. If you want to carry on connecting just once, without adding the key to the cache, hit No. If you do not trust this host, hit Cancel to abandon the connection.` where *<yyy:yyy:yyy:yyy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy>* are RSA key fingerprints of the server.	This message, or a similar message depending on the SSH client used, is normal and expected to appear at the first attempt to log on to a server.
`@@@

Message Example	Explanation
@@@@

5.3.3

Attaching Device to Serial Port

The Authentication Centre (AuC) external connection hosted by the serial port on the Core Server is shared with the Zone Controller (ZC) application server. Attaching the device to a serial port allows you to switch between the two applications, using iGAS menu.

NOTE: Only a single physical serial port is shared between AuC and ZC, the second serial port is reserved for AuC modem only.

Prerequisites: Log on as `instadm` using one of the following procedures:

- Logging On to the Server on page 106
- Logging On to iGAS Through a KVM Switch on page 108

Procedure:

1. Enter the number for **Application Device Management**.

   The **Application Device Management** menu appears:

   ```
   Application Device Management
   ----------------------------------------
   1. Display current device assignment
   2. Attach device to Application
   Please enter selection (1-2, q) [q]:
   ```

2. Enter the number for **Attach device to Application**.

   The **Attach device to Application** menu appears.

3. Enter the number for the application to which you want to attach the serial port.

   The port assignment changes and the **Application Device Management** menu appears.

4. To verify the current iGAS devices configuration, enter the number for **Display current device assignment**.

5.3.4

Provisioning Zone or Site Entity with an Infrastructure Key

When a Zone or Site is added to the System, the AuC synchronizes with UCS database and automatically generates an initial version of Infrastructure key (Ki) for each added Zone or BTS entity. The Ki is assigned to the entity in the AuC database. The assigned Ki should be delivered using a Key Variable Loader (KVL) to respective entity and the acknowledgment message should be returned via KVL to the AuC. When the Ki key is successfully provisioned the key Update can be enabled for the entity.

Prerequisites: Using iGAS menu, attach the device to serial port to operate with AuC application server. See Attaching Device to Serial Port on page 109.

Process:

1. Connect the KVL to the AuC server (directly or using a modem). Using the KVLs menu load the Ki from the AuC to KVL. See *DIMETRA KVL 4000 Air Interface Encryption and Authentication User Guide* for more information.

   The appropriate Ki keys are loaded to the KVL.

2. Do the following:

   - If you are provisioning the Ki to the Zone entity, connect the KVL to the Serial Port (to the left) of the Core Server (primary and standby) via the null-modem. Using the KVLs menu load the Ki from

the KVL to the ZC. Wait for the Ki to be uploaded to the ZC and for the acknowledgment message to be loaded back to the KVL.

- If you are provisioning the Ki to the BTS Site entity, follow Loading an Infrastructure Key (Ki) to a Site Entity on page 110.

3. Connect the KVL to the AuC server (directly or using a modem). Using the KVLs menu load the acknowledge messages form the KVL to the AuC. See *DIMETRA KVL 4000 Air Interface Encryption and Authentication User Guide* for more information.

   NOTE: If the Ki is loaded into a zone or Site entity, but the acknowledgment message is not returned to the AuC, this entity will not receive key updates which use Ki, that is, updates of KEKm and KEKz keys.

   The acknowledge messages are loaded to the AuC. The Ki **Status** becomes **Provisioned** for the selected Zone or Site entity. This signifies that the Ki key is successfully provisioned.

5.3.4.1

Loading an Infrastructure Key (Ki) to a Site Entity

Procedure:

1. If not already performed, configure the site according to system requirements.

   NOTE: Use a new configuration to create TSC configuration file (Do not use any other sites configuration file).

2. Commission the site for **local site trunking mode** (standalone mode) with the air interface encryption feature disabled in the site configuration file.
3. If the site has not yet been integrated with the DIMETRA system, commission the site for **wide area trunking mode** with air interface encryption feature disabled in the User Configuration Server (UCS).
4. Allow time for site configuration to be downloaded into the network management subsystem.

   NOTE: The site configuration must correctly specify the Zone ID and Site ID parameters. Otherwise, the KVL will download the wrong keys to the site. Use the TSCs Man-Machine Interface (MMI) to verify the correct Zone and Site IDs using the **display config** command.

5. Using a terminal interface, log in to the TSCs MMI using the FIELD login.

   You see the `SC>` prompt.

6. From Application Mode, type `LOCK` at the prompt.

   The BTS site is placed in locked mode.

7. Type `KVL` at the prompt.

   The front panel serial port is configured for KVL use.

8. Within 60 seconds, connect the KVL to the TSCs front serial port.
9. Using the KVL menus, load the Ki key into the TSC. See *DIMETRA KVL 4000 Air Interface Encryption and Authentication User Guide* for more information.

   Wait for the key load acknowledgment message.

10. Using a terminal interface, log in to the first Base Radio Controller (BRC) MMI using the FIELD login.

    You see the `BRC>` prompt.

11. Type `KVL` at the prompt.

    The front panel serial port is configured for KVL use.

12. Within 60 seconds, connect the KVL to the BRCs front serial port.
13. Using the KVL menus, load the Ki key into the BRC. See *DIMETRA KVL 4000 Air Interface Encryption and Authentication User Guide* for more information.

    Wait for the key load acknowledgment message.

14. Repeat step 10 through step 13 for each BRC at the BTS site.
15. Using a terminal interface, reconnect to the TSCs MMI using the FIELD login.

    You see the `SC>` prompt.

16. From Application Mode, type `UNLOCK` at the prompt.

    The BTS site is placed in unlocked mode.

17. Type `RESET` at the prompt to reset the TSC.

    The TSC is reset.

5.3.5
Reprovisioning Zone Entity with an Existing Infrastructure Key

In certain situations you may need to refresh existing Ki in a zone or Site entity, for example when a zone or Site entity is replaced by a new one or upgraded.

This task allows you to reprovision an existing Ki key to a zone or site entity. Perform this task when you want to reload a Ki key into the zone or site device, or when this is necessary because hardware at a site has been replaced.

Process:

1. In the AuC Client, select the zone or Site entity that requires Ki to be refreshed. Follow Refreshing a Ki for Selected Zone Entity on page 112 to refresh a Ki for a selected zone or site entity in the AuC Client.
2. Connect the Key Variable Loader (KVL) to the AuC server (directly or via a modem). Using the KVLs menu load the Ki from the AuC to KVL. See *DIMETRA KVL 4000 Air Interface Encryption and Authentication User Guide* for more information.

   The appropriate Ki keys are uploaded to the KVL.

3. Connect the KVL to the left serial port D of the primary ZC via the null-modem. Using the KVLs menu load the Ki from KVL to the ZC. Wait for the Ki to be uploaded to the Zone and for the acknowledgment message to be loaded back to the KVL.
4. Connect the KVL to the AuC server (directly or via a modem). Using the KVLs menu load the acknowledge messages from the KVL to AuC. See *DIMETRA KVL 4000 Air Interface Encryption and Authentication User Guide* for more information.

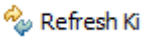
   The acknowledge messages are uploaded to the AuC. The Ki **Status** becomes **Provisioned** for the selected Zone or Site entity. This signifies that the Ki key is successfully reprovisioned.

5.3.5.1

Refreshing a Ki for Selected Zone Entity

Follow this procedure to refresh a Ki for selected zone entity in the AuC Client.

Procedure:

1. From the main AuC client window, select the **Devices** tab.
2. In the **Devices** tab, **Zones** pane, select the appropriate zone or BTS site in the.
3. Click the 

Refresh Ki button to re-provision an existing infrastructure key (Ki) for the selected entity.

   The Refresh Ki question appears.
4. Click **Yes**.

   The Refresh Ki information appears.
5. Click **OK**.

   The AuC is ready to upload the Ki to a KVL.

5.3.6

Reprovisioning Zone or Site Entity with a New Infrastructure Key

You may need to reprovision zone or Site entity with a new Ki key, for example when the Ki is believed to be compromised.

Process:

1. In the AuC Client select the zone or Site entity that requires new Ki to be assigned to. Follow Updating a Ki Key for a Zone or Site Entity on page 113 to update a Ki for selected zone or Site entity in the AuC Client.
2. Connect the Key Variable Loader (KVL) to the AuC server (directly or via modem). Using the KVLs menu load the Ki from the AuC to KVL. See *DIMETRA KVL 4000 Air Interface Encryption and Authentication User Guide* for more information.

   The appropriate Ki keys are uploaded to the KVL.
3. - If you are reprovisioning the new Ki to the Zone entity, connect the KVL to the Serial Port D of each Zone Controller (ZC) (primary and standby) via the null-modem. Using the KVLs menu load the Ki from the KVL to the ZC. Wait for the Ki to be uploaded to the Zone and for the acknowledgment message to be loaded back to the KVL.
   - If you are reprovisioning the new Ki to the Site entity, follow Loading an Infrastructure Key (Ki) to a Site Entity on page 110.

4. Connect the KVL to the AuC server (directly or via modem). Using the KVLs menu load the acknowledge messages from the KVL to the AuC. See *DIMETRA KVL 4000 Air Interface Encryption and Authentication User Guide* for more information.

   NOTE: If the Ki is loaded into a zone or Site entity, but the acknowledgment message is not returned to the AuC, the AuC will use the previous Ki for key updates which use Ki, that is, updates of KEKm and KEKz keys.

   The acknowledge messages are uploaded to the AuC. The Ki **Status** becomes **Provisioned** for the selected Zone or Site entity. This signifies that the Ki key is successfully reprovisioned.

5.3.6.1
Updating a Ki Key for a Zone or Site Entity

Follow the procedure below to update a Ki for a zone entity in the AuC Client.

Procedure:

1. From the AuC client main window, select the **Devices** tab.
2. In the **Devices** tab, **Zones** pane, select the appropriate zone or site .
3. Click the **Update Ki** Update Ki button to assign a new infrastructure key (Ki) for the selected entity.
4. In the **Update Ki** dialog box, click **Yes**.
5. In the **Update Ki** window, click **OK**.

   The Key Status icon becomes red for the selected zone or Site. This signifies that the new Ki key should be provisioned.

5.3.7
Clearing an Infrastructure Key from a Zone or BTS Site Entity

The Key Variable Loader (KVL) can clear (or "zeroize") an infrastructure key (Ki) from a zone or BTS site entity. This may be necessary when a zone device is decommissioned or permanently removed from service in the system.

For a BTS site, a Base Radio Controllers Ki key can also be zeroized through the BRC Man Machine Interface (MMI).

For information on performing this task with the KVL device, please refer to the *DIMETRA KVL 4000 Air Interface Encryption and Authentication User Guide*.

5.3.8
Scheduling Key Updates

The AuC manages updates of the following key types within the system infrastructure:

- system key encryption key (KEKm)
- session authentication material (SAI)
- zone key encryption key (KEKz)
- trunked mode static cipher key (TM-SCK)
- group session key for OTAR (GSKO)
- common cipher key (CCK)
- group cipher key (GCK)

- direct mode static cipher key (DM-SCK)

The **Schedules** tab in the Authentication Centre (AuC) Client allows you to manage key updates for system infrastructure entities. In particular it enables the following actions:

- configuring scheduled key updates
- performing immediate key updates
- enabling or disabling scheduled key updates based on a key type

When the AuC is part of a nationwide system, key schedules are shared by all the AuCs connected to it.

The following topics provide procedures associated with the **Schedules** tab in the AuC client display:

- Scheduling Key Updates on page 113
- Performing Immediate Key Updates on page 114
- Enabling/Disabling Key Updates By Key Type on page 120

The following topics provide reference information associated with the **Schedules** tab in the AuC client display:

- Key Schedule Information on page 45
- Key Schedules Selection on page 46

Follow the procedure below to schedule key updates for a key type throughout the system infrastructure.

Procedure:

1. From the AuC main client window, select the **Schedules** tab.
2. In the **Schedules** tab, **Key Schedules** pane, select the appropriate key type.

   The **Schedule Information** pane for the selected key type appears.
3. In the **Schedule Information** pane, select the date and the recurrence interval.

   NOTE: To set a new date and recurrence interval clear the Disable Key Schedules check box first. To go back to previous settings click **Revert** button.
4. Click **Apply**.

5.3.9
Performing Immediate Key Updates

The AuC manages updates of the following key types within the system infrastructure:

- system key encryption key (KEKm)
- session authentication material (SAI)
- zone key encryption key (KEKz)
- trunked mode static cipher key (TM-SCK)
- common cipher key (CCK)
- group session key for OTAR (GSKO)
- group cipher key (GCK)

- direct mode static cipher key (DM-SCK)

NOTE: Although the AuC may have completed a requested SCK or CCK change, the actual change on the air interface may not yet be complete (if the notification period has not yet expired). However, no harm will result if further key changes are requested - the site will initiate a change for the last activated key as soon as the ongoing change has completed.

Follow the procedure below to perform immediate key updates for a key type throughout the system infrastructure.

Procedure:

1. From the AuC main client window, select the **Schedules** tab.
2. In the **Schedules** tab, **Key Schedules** pane, select the appropriate key type.
3. In the **Schedule Information** pane, click **Start Update Now**.

   NationWide Only When the AuC is a part of a Nationwide system, key update is executed on every AuC that is a part of the Nationwide system.

   NOTE:
   You are prompted for confirmation because some updates may take a long time.

   Starting a manual update has no impact on the date and time for the next scheduled update.
4. Click **Yes**.

   NOTE: Each key contains threshold settings. Threshold settings are used for setting up a minimal value of performed updates that must be reached before another update can be sent out. However even if the threshold is reached the AuC will try to send the update to all available BTS . In nationwide mode, there is information shown that the threshold was reached, however before the next update can be sent out the other AuC's in the nationwide mode must fulfill their thresholds.

5.3.10
Assigning New Authentication Material for a Radio

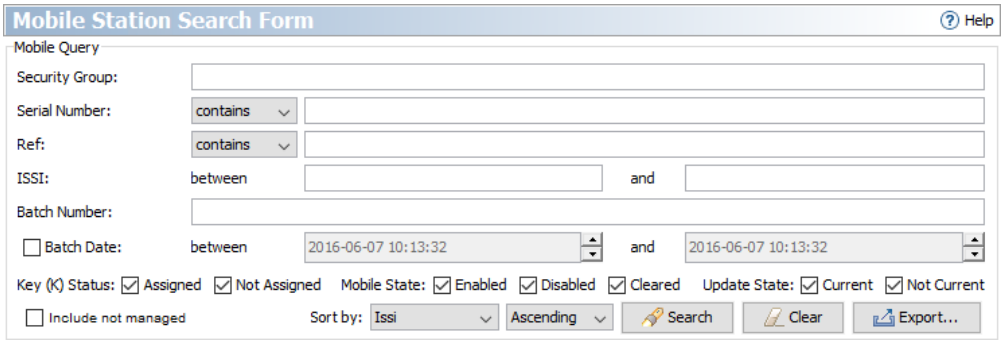
The AuC does not automatically assign authentication material for a radio when initially provisioned in the AuC database. You need to specifically select the Mobile Station (MS) to enable the MS for key updates.

WARNING: Once provisioned, and enabled for key updates future authentication material updates for an MS are performed during scheduled updates.

Procedure:

1. Select the **Mobiles** tab.
2. In the **Mobiles** tab, define the appropriate search criteria in the **Mobile Station Search Form**, highlighted below (search text is case-insensitive).

Figure 39: Mobile Station Search Form - Example



NOTE: You must specify the appropriate security group in order to execute a radio search. You can select a security group from the **Security Groups** tree display and the entry is automatically populated in the **Security Group** field.

The radio selection(s) are highlighted.

3. Click on the **Search** button. The search results are displayed in the list window.
4. Select the appropriate radio(s) in the list window. To select multiple MSs, do the following:
   - To select a group of MSs that are next to each other in the list window, click and drag the mouse over the selections (or hold down the SHIFT key and click each item you want to select).
   - To select a group of MSs that are not next to each other in the list window, hold down the CTRL key and click each item you want to select.

   The radio selection(s) are highlighted.
5. To update authentication material and GSKO for the selected MSs, click the **Resend** button.
6. To disable Mobile key updates for the selected MSs, click the **Disable** button.
7. Click **Yes**.

   The information is saved in the AuC database.

5.3.11
Reversing USB Order

If Authentication Centre (AuC) is hosted on a server with USB-to-serial adapters, it may be required to reverse the USB order to use a specific port with Key Variable Loader (KVL) or AuC modem.

If you failed to connect KVL/AuC modem using a specific USB port, perform the following procedure.

Prerequisites:

Disconnect the KVL/AuC modem.

Leave the USB-to-serial adapter(s) plugged in to the server.

Procedure:

1. Log on to iGAS as `instadm` by using one of the following procedures:
   - Logging On to the Server on page 106
   - Logging On to iGAS Through a KVM Switch on page 108
2. In the **Installation Administrator Main Menu**, enter the number for **Application Device Management**.
3. In the **Application Device Management** screen, enter the number for **Reverse USB order**.

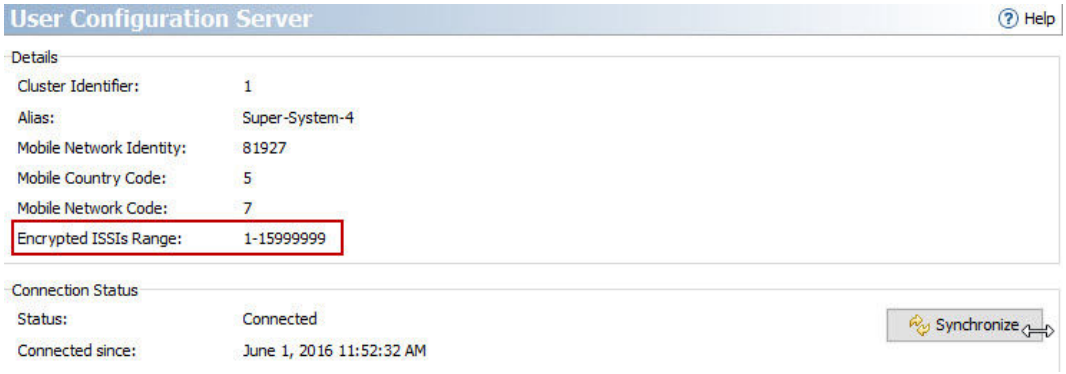
4. Reconnect the KVL/AuC modem.

5.4 Clearing a Radio

Procedure:

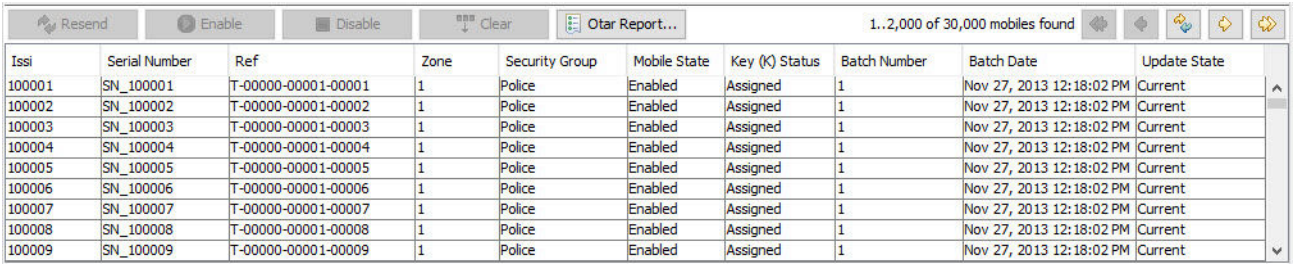
1. Select the **Synchronization** tab.
2. In the **Synchronization** tab, check the Encrypted ISSIs range.

   Figure 40: Full Synchronization with UCS - Example



3. Select the **Mobiles** tab.
4. In the **Mobiles** tab, select the appropriate radio(s) in the list window. To select multiple MSs, do the following:
   - To select a group of MSs that are next to each other in the list window, click and drag the mouse over the selections (or hold down the **SHIFT** key and click each item you want to select).
   - To select a group of MSs that are not next to each other in the list window, hold down the **CTRL** key and click each item you want to select.

   Figure 41: Mobiles List - Example



Issi	Serial Number	Ref	Zone	Security Group	Mobile State	Key (K) Status	Batch Number	Batch Date	Update State
100001	SN_100001	T-00000-00001-00001	1	Police	Enabled	Assigned	1	Nov 27, 2013 12:18:02 PM	Current
100002	SN_100002	T-00000-00001-00002	1	Police	Enabled	Assigned	1	Nov 27, 2013 12:18:02 PM	Current
100003	SN_100003	T-00000-00001-00003	1	Police	Enabled	Assigned	1	Nov 27, 2013 12:18:02 PM	Current
100004	SN_100004	T-00000-00001-00004	1	Police	Enabled	Assigned	1	Nov 27, 2013 12:18:02 PM	Current
100005	SN_100005	T-00000-00001-00005	1	Police	Enabled	Assigned	1	Nov 27, 2013 12:18:02 PM	Current
100006	SN_100006	T-00000-00001-00006	1	Police	Enabled	Assigned	1	Nov 27, 2013 12:18:02 PM	Current
100007	SN_100007	T-00000-00001-00007	1	Police	Enabled	Assigned	1	Nov 27, 2013 12:18:02 PM	Current
100008	SN_100008	T-00000-00001-00008	1	Police	Enabled	Assigned	1	Nov 27, 2013 12:18:02 PM	Current
100009	SN_100009	T-00000-00001-00009	1	Police	Enabled	Assigned	1	Nov 27, 2013 12:18:02 PM	Current

5. Click **Clear**, then click **Yes** twice to confirm.

   Cleared radio(s) appear on the list window in cleared state.

5.5 Enabling and Disabling Key Updates

- Entity Status and Key Information on page 85
- Entering and Modifying Keys on page 94
- Key Distribution on page 106

5.5.1

Enabling/Disabling Key Updates for a Radio

The AuC manages updates of authentication material, common cipher keys (CCK), and static cipher key-trunked mode operation (SCK-TMO) keys in the system infrastructure. Using the AuC, you can select to enable or disable future updates of keys that relate to specific radios.

IMPORTANT: A disabled MS will not be allowed to access to the system if authentication is enabled.

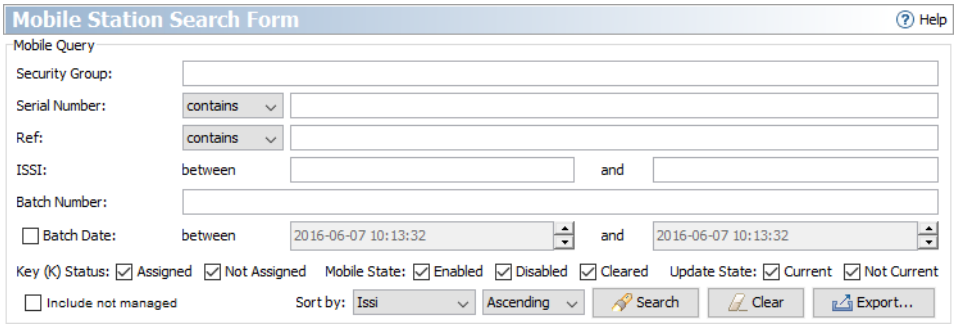
WARNING: A device should only be disabled for key updates if considered non-operational. Similarly, a device should only be enabled for key updates if operational.

Follow the procedure below to enable or disable key updates for a radio.

Procedure:

1. Select the **Mobiles** tab.
2. In the **Mobiles** tab, **Mobile Station Search Form** pane, define the appropriate search criteria, as highlighted below (search text is case-sensitive).

   Figure 42: Mobile Station Search Form - Example



   NOTE: You must specify the appropriate security group in order to execute a radios search. You can select a security group from the **Security Groups** tree display and the entry is automatically populated in the **Security Group** field.

   The radios selection(s) are highlighted.

3. Click **Search**.

   The search results are displayed in the list window, highlighted below.

4. Select the appropriate radio(s) in the list window. To select multiple MSs, do the following:
   - To select a group of MSs that are next to each other in the list window, click and drag the mouse over the selections (or hold down the SHIFT key and click each item you want to select).
   - To select a group of MSs that are not next to each other in the list window, hold down the CTRL key and click each item you want to select.

   The radio selection(s) are highlighted.

5. To enable Mobile key updates for the selected MSs, click the **Enable** button.

   The **Mobile State** field in the list window is changed to "Enabled".

6. To disable Mobile key updates for the selected MSs, click the **Disable** button.
7. In the **Disable Mobile Key Updates**, click **Yes**.

   The Mobile State field in the list window is changed to "Disabled (manually)".

5.5.2
Enabling/Disabling Key Updates for a Zone

The AuC manages updates of zone entities in the system infrastructure. Using the AuC, you can select to enable or disable future key updates (scheduled and on demand) relating to a specific zone entity.

Follow the procedure below to enable or disable key updates for a zone.

Procedure:

1. From the AuC client main window, select the **Devices** tab.
2. In the **Devices** tab, **Zones** pane, locate and select the appropriate zone.
3. Locate and click on the appropriate zone in the **Zones** tree display on the left.
4. Click the **Enable** button to enable or **Disable** button to disable key updates for the selected zone. The location of the button is highlighted below.

   NOTE: The Key Updates button is a toggle button. Thus, when Key Updates are enabled, the button will say **Disable**, and when Key Updates are disabled, it will say **Enable**.

   The status of a zone and all sites beneath changes accordingly. If key updates are being disabled, a confirmation dialog box appears.

5.5.3
Enabling/Disabling Key Updates for a Site

The AuC manages key updates for sites in the system infrastructure. Using the AuC, you can select to enable or disable future key updates (scheduled and on demand) relating to a specific site. Site key updates status can be modified only when key updates are enabled for the zone which the site belongs to.

When a new site is added into the AuC it is in the disabled state by default. You can manually enable the site when either a Ki is provisioned for this site or a DIMETRA Distribution Key (DDK) is configured.

Follow the procedure below to enable or disable key updates for a BTS site.

Procedure:

1. From the AuC client main window, select the **Devices** tab.
2. In the **Devices** tab, **Zones** pane, locate and select the appropriate site.
3. In the **Site Detailed View** tab, click the **Enable** button to enable or **Disable** button to disable key updates for the selected BTS site. The location of the button is highlighted below.

   NOTE: The Key Updates button is a toggle button. Thus, when Key Updates are enabled, the button will say **Disable**, and when Key Updates are disabled, it will say **Enable**.

   The status of the site changes accordingly. If key updates are being disabled, a confirmation dialog box appears.

5.5.4
Resetting a Site

Follow the procedure below to reset a BTS site.

Procedure:

1. From the AuC client main window, select the **Devices** tab.
2. In the **Devices** tab, **Zones** pane, select the appropriate site.

3. In the **Site Detailed View** pane, click **Reset** to reset selected site.
4. In the confirmation dialog box, enter a reason for resetting the site and click **OK**.

   IMPORTANT:
   Pressing **OK** in the **Reset Site Window** removes all keys from the site except Ki!
   The site automatically retrieves the current keys form the AuC after the reset.

   Status of a Site is displayed in the Events pane.

5.5.5 Enabling/Disabling Key Updates By Key Type

Follow the procedure below to enable or disable scheduled key updates for a key type throughout the system infrastructure.

NOTE: This procedure affects scheduled updates only (immediate key updates can still be performed). When disabling, any key updates currently in progress will continue to be performed.

Procedure:

1. From the AuC main client window, select the **Schedules** tab.

   The **Schedules** tabbed pane appears.

2. In the **Key Schedules** display, locate and click on the appropriate key type .
3. To enable key updates, clear **Disable Key Schedule** check box, select appropriate date.

   Your schedule information is stored and a key update takes place when scheduled.

4. To disable key updates, select **Disable Key Schedule**.

   The **Modify Schedule** window closes and the **Key Schedule State** shows **Disabled**.

5. To accept all the changes, click **Apply**.

5.5.6 Enabling/Disabling KVL Access to the Authentication Centre

The Authentication Centre (AuC) allows you to control a key variable loaders (KVL) access to the AuC. A KVL must be allowed access to perform transfer of infrastructure keys (Ki) to system entities.

Procedure:

1. From the AuC client main window, select the **KVLs** tab.

   The **KVLs** tabbed pane appears.

2. Select a KVL from the **KVLs** list display.

   The KVLs key information appears in the work pane.

3. To enable or disable KVL access to the AuC, click the **Deny Access/Allow Access** button.

   NOTE: The **Deny Access/Allow Access** button is a toggle button. Thus, you click the same button to turn KVL access on or off. For example, to enable KVL access (when disabled) to the AuC, you click the **Allow Access** button. Once KVL access is enabled, the toggle buttons state changes to **Allow Access**. This allows you to disable KVL access to the AuC in the future.

   The KVLs current key status is changed in both the colored icon of the **KVLs** display and by the **Status** field in the **KVL Information** display. If KVL access is being disabled, the following dialog box appears.

4. Click **Yes**.

   The KVLs current key status is changed to disabled in both the colored icon of the **Key Status** display (to red) and by the **Status** field in the KVL Information display.

Chapter 6

Crypto Management Group Configuration

6.1 Importing Mapping Files

Procedure:

1. Select the **CMGs** tab.

   The **CMGs** tabbed pane appears.

2. Select the **Mappings** tab on the left.

   The **Mappings** tabbed pane appears.

3. Click the **Import mappings into the selected configuration** button.

   The **Select files to import** window appears.

4. Click the **Add** button.

   The **Open** window appears.

5. In the **Open** window select the mapping files you want to import and click **Open**.

   The **Open window** closes and the list of files to import appears in the **Select files to import** window.

6. Click the **Next** button to see the status of the CMG configuration files.

   The **Select files to import** window appears. The status of the CMG configuration files is displayed.

7. Click the **Next** button to go to the next step.

   NOTE: If there are any conflicts you should resolve them on the Hierarchy tab in the wizard window. The conflicts can be resolved by removing or disabling CMGs, removing operational groups, ISSI or GSSI ranges. Please note that the Hierarchy view on the wizard can be used in the the same way as the Hierarchy or Edited Hierarchy views on the CMGs tab.

   The **Select files to import** window appears.

8. Click the **Apply** button to validate imported data, then **Next** , and finally **Finish** to import the CMG mappings.

6.2 Exporting CMG Mappings

Procedure:

1. Select the **CMGs** tab.
2. In the **CMGs** tab, select the **Mappings** tab on the left.
3. Click the **Export mappings** button.
4. In the **Export Mappings** window, select the appropriate options and click **Browse**.

   The **Save** window appears.

5. In the **Save** window select the folder you wish to export the mappings to, click **Save** and than **OK**.

6.3 Enabling CMGs

After importing CMG Mapping files the CMGs are disabled. You can enable CMGs in the **CMGs** pane.

Procedure:

1. Select the **Hierarchy** tab on the left.
2. In the **CMGs** pane, select a CMG that you want to enable.
3. In the **CMG - Hierarchy**pane, select the **Active** check box.

   IMPORTANT: During the synchronization of CMG data a **CMG change ongoing** icon can be displayed on the **Status Bar**. While the operation takes place and the icon is being displayed the zones and sites can not synchronize keys (unless user allows it in **System Preferences**).

   The CMG is now active

6.4 Assigning GCKNs and KAGNs

Procedure:

1. In the CMGs tab click on the **Hierarchy** tab on the left.
2. In the **Hierarchy** tab, **CMGs** pane, select the appropriate TMO or DMO operational group.

   Operational Group Details are shown in the Work Pane

3. In the **CMG – Hierarchy** pane, select a GCKN you want to assign to the TMO operational group and click **Assign GCKN**. In case of a DMO operational group, select a KAGN you want to assign and click **Assign KAGN**.

   NOTE: You can assign GCKNs to TMO operational groups manually using the procedure above or automatically by clicking **Auto Assign GCKNs**. KAGNs can also be assigned automatically by clicking **Auto Assign KAGNs** button.

   The number is assigned to an operational group.

6.5 Creating CMGs

Procedure:

1. Select the **CMGs** tab.
2. In the **CMGs** tab, left-hand side, select the **Hierarchy** tab.

   The **Hierarchy** tabbed pane appears.

3. In the **CMGs** selection display click the **Create CMG** button ( ).
4. In the **Add CMG** window, enter the name for the CMG that you want to create. Click **OK**.

   New CMG appears in the **CMGs** display.

5. Create ISSI ranges for the newly-created CMGs. See Creating ISSI Ranges on page 124

6.6 Removing CMGs

Procedure:

1. Select the **Hierarchy** tab on the left.

   The **Hierarchy** tabbed pane appears.

2. In the **CMGs** selection display, select the CMG you want to remove and perform Removing ISSI Ranges on page 124 in order to remove ISSI ranges for this CMG.
3. In the **CMGs** selection display, click the **Remove CMG** button ( ).
4. In the **Confirm CMG Remove** window click **Yes** to delete the CMG.

6.7 Creating ISSI Ranges

Procedure:

1. Select the **Hierarchy** tab on the left.

   The **Hierarchy** tabbed pane appears.

2. Click the **Add ISSI Range** button in the **ISSI Ranges** pane.
3. In the **New Range** window enter the range bounds for the CMG and click **OK**.

6.8 Removing ISSI Ranges

Procedure:

1. Select the **Hierarchy** tab on the left.
2. In the **CMGs** pane, select a CMG for which you want to remove the ISSI ranges.
3. In the **ISSI Ranges** pane, select the ISSI Range that you want to remove.
4. Click the **Remove ISSI Range** button.
5. In the **Confirm ISSI Range Remove** window, click **Yes**.

6.9 Creating Operational Groups

Procedure:

1. Select the **CMGs** tab.
2. In the **CMGs** tab, left-hand side, select the **Hierarchy** tab.

   The **Hierarchy** tabbed pane appears.

3. In the **CMGs** pane, select the CMG in which you want to create the Operational Group. Click the **Create Operational Group** button.

   Add Operational Group window appears.

4. In the **Add Operational Group** window enter the name for the Operational Group, select its type and click **OK** to create it.

6.10 Removing Operational Groups

Procedure:

1. Select the **Hierarchy** tab on the left.
2. In the **CMGs** pane, select the Operational Group you want to remove and click the **Remove Operational Group** button.

   The Confirm Operational Group Remove window appears.

3. In the **Confirm Operational Group Remove** window click **Yes** to remove the Operational Group.

6.11 Creating GSSI Ranges

Procedure:

1. Select the **CMGs** tab.
2. In the **CMGs** tab, left-hand side, select the **Hierarchy** tab.

   The **Hierarchy** tabbed pane appears.

3. In the **GSSI Ranges** pane, select the desired group. Click the **Add GSSI Range** button in the **GSSI Ranges** pane.
4. In the **New Range** window, enter the range bounds for the selected group. Click **OK**.

6.12 Removing GSSI Ranges

Procedure:

1. Select the **Hierarchy** tab on the left.
2. In the **Hierarchy** tab, **CMGs** pane on the left, select a group for which you want to remove the GSSI ranges.
3. In the **GSSI Ranges** pane, select the GSSI Range that you want to remove.
4. Click the **Remove GSSI Range** button.
5. In the **Confirm GSSI Range Remove** window click **Yes**.

6.13 Enabling CMG Configuration

Procedure:

1. Select the **Hierarchy** tab on the left.
2. In the **Hierarchy** tab, **CMGs** pane on the left click the **Enable Configuration** button.

   IMPORTANT: In order to enable configuration all of the operational groups in enabled CMGs must have GCKNs or KAGNs assigned.

   The Enable CMG Configuration window appears.
3. In the **Enable CMG Configuration** window click **Yes**.

   IMPORTANT: During the synchronization of CMG data a **CMG change ongoing** icon can be displayed on the **Status Bar**. While the operation takes place and the icon is being displayed the zones and sites can not synchronize keys(unless user allows it in the **System Preferences**).

   The CMG Configuration is now enabled.

6.14 Editing Enabled CMG Configuration

After enabling the CMG configuration it is impossible to update the configuration on the Hierarchy tab. If you wish to update the CMG configuration perform procedure below.

IMPORTANT: Do not configure Nationwide while editing CMG Configuration. Before configuring Nationwide apply or cancel changes made on the **Edited Hierarchy** tab.

Procedure:

1. Select the **Hierarchy** tab on the left.
2. In the **CMG Hierarchy** pane on the right click the **Edit CMGs** button.

   New tab appears on the left.
3. Select the **Edited Hierarchy** tab. Then, you can update the CMG configuration in a similar way as on the **Hierarchy** tab before enabling the CMG configuration.
4. After updating the CMG configuration click **Apply Updates** button in the **CMG Edited Hierarchy** display.

   IMPORTANT: During the synchronization of CMG data a **CMG change ongoing** icon can be displayed on the status bar. While the operation takes place and the icon is being displayed the zones and sites can not synchronize keys (unless user allows it in the **System Preferences**).

   CMG configuration is updated. The **Edited Hierarchy** tab disappears.

6.15 Disabling CMG Configuration

Procedure:

1. Select the **CMGs** tab.
2. In the **CMGs** tab, left-hand side, select the **Hierarchy** tab.

3. In the **CMGs** pane on the left select click the **Disable Configuration** button.

   IMPORTANT: The configuration must be empty before disabling it.

   The Disable CMG Configuration window appears.

4. In the **Disable CMG Configuration** window click **Yes**.

   IMPORTANT: During the synchronization of CMG data a **CMG change ongoing** icon can be displayed on the **Status Bar**. While the operation takes place and the icon is being displayed the zones and sites can not synchronize keys(unless user allows it in the **System Preferences**).

   The CMG Configuration is now disabled.

6.16 OTAR Configuration

Procedure:

1. Select the **CMGs** tab.
2. In the **CMGs** tab, select the **CMG Keys** tab on the left.

   The **CMG Keys** tabbed pane appears.

3. In the **CMG Keys Details** window click the **Enable OTAR** button for the GSKO key.

   NOTE: After enabling OTAR for GSKO it will be possible for you to enable OTAR for other keys by clicking **Enable OTAR** button situated by keys name.

   IMPORTANT: During the synchronization of CMG data a **CMG change ongoing** icon can be displayed on the **Status Bar**. While the operation takes place and the icon is being displayed the zones and sites can not synchronize keys(unless user allows it in the **System Preferences**).

   OTAR will be enabled for the GSKO key. Other **Enable OTAR** buttons become active.

6.17 Disabling OTAR

Procedure:

1. In the **CMGs** tab, select the **CMG Keys** tab on the left.

   The **CMG Keys** tabbed pane appears.

2. In the **CMG Keys Details** pane, click the **Disable OTAR** button for the key that you want to disable.

   IMPORTANT: You must first disable OTAR for DM-SCK, GCK and TM-SCK keys only then you will be able to disable OTAR for GSKO.

   IMPORTANT: During the synchronization of CMG data a **CMG change ongoing** icon can be displayed on the **Status Bar**. While the operation takes place and the icon is being displayed the zones and sites can not synchronize keys(unless user allows it in the **System Preferences**).

   OTAR is disabled for the selected key.

Chapter 7

Nationwide AuC Configuration

For a nationwide (multicluster) DIMETRA system, an AuC is required for each cluster (each cluster supports up to seven zones). Each AuC handles the key management tasks for that cluster. To support system-wide key management tasks, the AuCs in the nationwide system communicate with one another to perform updates of the KEKm, TM-SCK, CCK, GSKO, GCK and DM-SCK keys. The nationwide AuC system consists of one Master AuC and up to seven Slave AuCs. It has to be manually configured which of the AuCs is a Master AuC. Master AuC is responsible for following operations:

- assuring that system-wide keys in all AuCs in the nationwide system are consistent
- initiating nationwide key updates of system-wide keys
- coordinating updates between the Slave AuCs
- coordinating update schedules between the Slave AuCs

The system-wide keys are transferred securely between AuCs using a shared AuC communication key (AuC Comm Key).

IMPORTANT: Do not configure Nationwide while editing CMG Configuration. Before configuring Nationwide apply or cancel changes made on the **Edited Hierarchy** tab.

7.1 Viewing AuC Connection Information and Status

The **Nationwide** tab in the Authentication Centre provides information about the nationwide system that the local AuC is part of.

NOTE: If the AuC is not part of the nationwide system, the **Nationwide** tab is not displayed and therefore cannot be selected.

The local AuC is the AuC, which the user is currently logged onto. For each AuC Server listed in the **AuC Net** window, the **AuC Connectivity** pane provides the following information:

- Server Alias
- Server ID
- Server Version
- Server Status
- Nationwide Role
- IP Address

If you are logged to the Master AuC Server then you will be provided with additional information about the key update status for the following keys:

- CCK
- KEKm
- TM-SCK
- DM-SCK
- GCK
- GSKO

When the AuC is part of the nationwide system, follow procedure below to view connectivity status and information about the nationwide system.

Procedure:

1. From the AuC client main window, select the **Nationwide** tab.

   If the AuC is a part of nationwide system you can see the system structure in the **AuC Net** pane. The Master AuC is displayed in green while all the AuC slave servers are displayed in blue. For the explanations of the servers icons see Table 7: AuC Server Status Information and Icons on page 37.

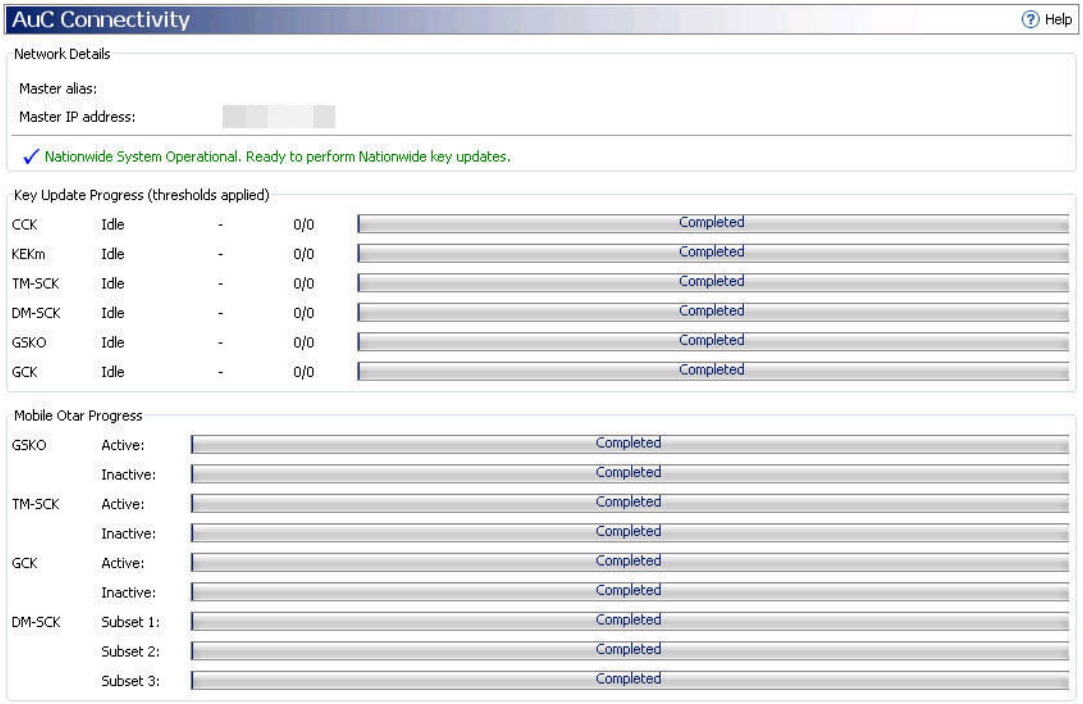
   In the **AuC Connectivity** pane information about the nationwide AuC system is displayed (see Table 21: Fields in the AuC Connectivity Information Display on page 42 for details).

   The AuC server that you are currently logged on, is displayed with the status **In-Service**.

   Figure 43: AuC Net Pane Example

2. In the **AuC Net** pane, select the AuC Server you wish to see information about. The information is displayed in the **AuC Connectivity** pane (see Table 6: Fields in the AuC Connectivity Information Display on page 35 for details).

Figure 44: AuC Connectivity Pane Example



- If the local AuC is a nationwide master, the information about selected AuC Server Alias, ID, Version, Status, Nationwide Role, IP Address and key update status is displayed. If the key update is locked on the selected AuC, information about it is also provided.
- If the local AuC is a nationwide slave, the information about selected AuC Server Alias, ID, Version, Status, Nationwide Role and IP Address is displayed.

7.2 Nationwide AuC System Configuration

The following process describes the configuration of the nationwide AuC system.

Prerequisites:

- All AuC Servers that will be connected to the nationwide system have the same AuC Comm Key.
- There is no key update in progress.
- All AuC Serves that will be connected to the nationwide system have the same SCK Table.
- The time set on the AuC Servers cannot vary more than 5 minutes.
- The encryption devices are provisioned with the same **System Key.**
  The **DVI_XL Key** (also referred to as **Master Key**) can differ between instances. See Encryption Device Configuration on page 143 for more details.

NOTE: If you receive the `Signature mismatch` error during the process, verify that the AuC Comm Key is the same for all AuC instances connected to the nationwide system. Also ensure that the encryption device is provisioned with the same system key.

Process:

1. Choose the AuC Server to be the nationwide master and configure it according to Configuring Nationwide Master AuC on page 131.

   NOTE: Choose one of the remaining AuC Servers to be the Expected Slave.

2. Configure the AuC Server configured on master to be Expected Slave as a nationwide slave according to Configuring Nationwide Slave AuC on page 132.
3. To add more nationwide slaves to the network:Repeat this step until all slaves will be added.
   a. Wait for the nationwide master to synchronize keys. The key update status in the **AuC Connectivity** window should be **Idle** for all keys.
   b. Set Expected Slave on the nationwide master according to Adding a New Slave AuC to the Nationwide System on page 135.
   c. Configure the AuC Server chosen to be Expected Slave as a nationwide slave, according to Configuring Nationwide Slave AuC on page 132.

   NOTE: When this process is completed, the KEKm, TM-SCK, CCK, GSKO, GCK and DM-SCK keys and their update schedules for all AuC Servers connected to the nationwide system, will be synchronized by the nationwide master.

7.2.1
Configuring Nationwide Master AuC

Procedure:

1. From the main AuC Client menu select **Nationwide** → **Become Master**.

   You are prompted for IP address of Expected Slave AuC.

2. Enter the IP address of Expected Slave AuC and press **OK**.
3. Select the **Nationwide** tab.

   The **Nationwide** tabbed pane is displayed. The Slave AuC is listed in the **AuC Net** pane as **Expected**.

4. Wait until the Expected Slave AuC connects to the AuC Net.

   NOTE: Only AuC with the IP address matching the IP address of the Expected Slave defined in step 2 will be able to connect to the Master AuC. To change the IP address of the Expected Slave, see Changing Expected Slave AuC on page 135. To learn how to configure Slave AuC and connect it to the system, see Configuring Nationwide Slave AuC on page 132.

Figure 45: AuC Net Pane Example

When the Expected Slave AuC connects to the AuC System it will be listed in the **AuC Net** pane as **Connected**. Master will automatically update the CCK, SCK-TMO and System KEK keys on the Slave AuC.

5. To add more Slave AuCs to the net, see Adding a New Slave AuC to the Nationwide System on page 135.

   NOTE: There can be up to seven Slave AuCs in the Nationwide system.

7.2.2 Configuring Nationwide Slave AuC

Procedure:

1. From the **Nationwide** menu select **Become Slave**.

   You are prompted for IP address of Master AuC.

2. Enter the IP address of Master AuC and press **OK**.

   The Master AuC and the Slave AuC are listed in the **AuC Net**. Initially the status of the Master AuC is **Connecting...**

3. Wait until the Slave AuC connects to the Master AuC. The slave will be able to connect to the Master AuC only when its IP address is set in the Master AuC as the IP address of the Expected Slave AuC.

   NOTE: When the attempt to connect to the Master AuC fails, one of the following messages appears in master's **Event Log**:

   - `Connection closed. Reason (Unknown Address)` - IP address of the Expected Slave AuC set up in Master AuC does not match the IP address of Slave AuC that is trying to connect;
   - `Connection closed. Reason (Different Static Cipher Key Table)` - the SCK tables on master and slave do not match;
   - `Connection closed. Reason (Authentication Failure - Signature Mismatch)` - the CommKeys on master and slave do not match;
   - `Connection closed. Reason (Authentication Failure - Unacceptable Time Difference)` - the time difference between servers is greater than 5 minutes;

Figure 46: AuC Net Pane Example

The Slave AuC tries to establish the connection with the master every 5 minutes until it succeeds. When the Slave AuC connects to the master, the status of the master listed in the **AuC Net** pane changes to **Connected**.

4. The KEKm, TM-SCK, CCK, GSKO, GCK and DM-SCK keys in connected Slave AuC and/or other AuC Servers will be updated, so that as the result they are identical. When the key update fails, there is one of the messages listed and described in Table 97: Rejected Key Update Event Log Messages on page 133 in masters **Event Log**. See the description of the received message to find the solution and enable the key update.

7.2.3
Rejected Key Update Event Log Messages

Table 97: Rejected Key Update Event Log Messages

Reason Field	Description
Key update in progress	The key update is already in progress. Wait until it finishes.
Key updates disabled	The key update has been disabled on one of the AuC Servers in the nationwide network. Make sure that the key update is unlocked on every AuC Server in nationwide network to enable the Master AuC to execute automatic key update.
Not all servers connected	Not all AuC Serves in the nationwide system are currently connected to the network. Restore the connection to proceed with key update.
Invalid network configuration	There is only one server in the AuC Network. The nationwide key update can be executed only in multicluster system.
Remote server data missing	The Master AuC doesnt have information about slavess keys. Please wait until the Master AuC receives the information.
Decryption failure	The decryption failed. Check if the CommKeys in Slave AuC and Master AuC match each other.

Reason Field	Description
UCS disconnected	The AuC has been disconnected form the UCS. Restore the connection with UCS.
Remote server did not respond in time	AuC Server did not answer for key update request within one minute.

7.3 Key Updates in the Nationwide System

NOTE: The following steps are performed automatically by the Master and Slaves AuCs. No action from the user is required. The process is presented only for information purposes.

Process:

1. Master AuC checks the following preconditions:

   All AuC servers must be connected to the nationwide system
   Key updates on all AuC servers must be unlocked
   There must not be any key updates in progress

2. Master AuC sends inquiry to all AuC servers that take part in the key update to check if the key update can be started.
3. Slave AuCs respond to Master AuC. The response can be either positive or negative. When the response is negative the Slave AuC provides the Master AuC with the reason of rejection, see Table 97: Rejected Key Update Event Log Messages on page 133. If the key update is rejected by the Slave AuC then, depending on the update type Master AuC performs the following actions:

   NOTE: For the Master AuC SW Release 5.5 (or higher) and the Slave AuC SW Release 5.2 (or lower) the reason of update rejection is always Unknown.

   - If it is **immediate key update**, the update will not be executed
   - If it is **scheduled key update**, Master AuC repeats the request in one hour time intervals, until the response is positive. When the responses from all AuC Slaves are positive, the key update starts.
   - If it is **initial synchronization**, Master AuC repeats the request in five minutes time intervals, until the response is positive. When the responses from all AuC Slaves are positive, the key update starts.

4. During the key update, the Slaves AuCs send their current status information to Master AuC. On this basis Master AuC generates summary report, which can be viewed in the **AuC Connectivity** tab. For more information see, Viewing AuC Connection Information and Status on page 128.
5. When specific stage of key update is completed on each AuC server (the progress reaches 100%) Master AuC decides to start the next stage. Master AuC sends a request to start the next stage to each AuC Slave.
6. Slave AuCs respond to Master AuC. The response can be either positive or negative. If the slaves response is negative, Master AuC repeats its request every 5 minutes (Exception: if synchronizing with UCS is the reason of rejection, Master AuC repeats its request every 30 seconds). When the response is positive, Master AuC sends a command to move to the next update stage to all Slave AuCs.
7. When all stages of the key update are completed, the key update process is finished.

7.4 Slave AuCs Reconfiguration in the Nationwide System

In the Master AuC, you can introduce the following changes into the Slave AuCs configuration:

- Add new Slave AuC to the AuC System, see Adding a New Slave AuC to the Nationwide System on page 135.
- Change Expected Slave AuC, see Changing Expected Slave AuC on page 135.
- Remove Expected Slave AuC from the AuC System, see Removing Expected Slave AuC on page 135
- Remove Slave AuC from the AuC System, see Removing Slave AuC from the Nationwide System on page 136.

7.4.1
Adding a New Slave AuC to the Nationwide System

Procedure:

1. On the Master AuC select the **Nationwide** tab from the AuC client main window.

   The **Nationwide** tabbed pane appears.

2. From the main AuC Client menu select **Nationwide** → **Add Expected Slave...**.

   You are prompted for IP address of Expected Slave AuC.

3. Insert the IP address of Expected Slave AuC and press **OK**.

   The Slave AuC is listed in the **AuC Net** window as **Expected**.

4. Wait until the Expected Slave AuC connects to the AuC Net.

   NOTE: Only AuC with the IP address matching the IP address of the Expected Slave defined in step 3 will be able to connect to the AuC Net. To change the IP address of the Expected Slave, see Changing Expected Slave AuC on page 135. To learn how to configure Slave AuC and connect it to the system, see Configuring Nationwide Slave AuC on page 132.

   When the Expected Slave AuC connects to the AuC System it will be listed in the **AuC Net** window as a **Connected**.

7.4.2
Changing Expected Slave AuC

Procedure:

1. From the main AuC Client menu select **Nationwide** → **Change Expected Slave**.

   You are prompted for IP address of Expected Slave AuC.

2. Insert the IP address of the new Expected Slave AuC and press **OK**.

   The new Slave AuC is listed in the **AuC Net** window as **Expected**.

7.4.3
Removing Expected Slave AuC

Procedure:

1. From the AuC client main window, select the **AuC Connectivity** tab.

   The **AuC Connectivity** tabbed pane appears.

2. From the main AuC Client menu select **Nationwide** → **Remove Expected Slave**.

   NOTE: This option is available only when at least one Slave AuC is connected to the Master AuC.

   The Expected Slave AuC is deleted from the **AuC Net** window.

7.4.4
Removing Slave AuC from the Nationwide System

Follow the procedure below to remove Slave AuC from the nationwide system.

IMPORTANT: Removing an AuC from the nationwide network means that this AuC will no longer participate in nationwide key updates. If it is still desired for the radios located in this AuCs cluster to maintain communication with MSs in other clusters, removing the AuC is **NOT** recommended. Failure to follow this recommendation may result in loss of radio communication between the cluster that has been removed and the remaining clusters in the nationwide network.

Procedure:

1. On the Master AuC select the **Nationwide** tab from the AuC client main window.

   The **Nationwide** tabbed pane appears.

2. From the main AuC Client menu select **Nationwide** → **Remove Slave**.

   You are prompted for IP address of the Slave AuC to be removed.

3. Insert the IP address of Slave AuC to be removed and press **OK**.

   NOTE: Only disconnected Slave AuC can be removed.

   The Slave AuC is delisted from the AuC System. It is reflected in the **AuC Net** window.

7.5
Returning to the Single Cluster Mode

Procedure:

1. On the Master AuC select the **Nationwide** tab from the AuC client main window.

   The Nationwide tabbed pane appears.

2. Remove all Slave AuCs. To remove Slave AuC follow Removing Slave AuC from the Nationwide System on page 136.

   NOTE: The Expected Slave AuC does not need to be removed.

3. From the main AuC Client menu select **Nationwide** → **Back To Single Cluster**.

   The **AuC Net** window becomes empty.

7.6
Nationwide AuC System Reconfiguration

To reconfigure nationwide AuC system you can:

- connect Slave AuC to another Master AuC, see Connecting Slave AuC to Another Master on page 137.

- change nationwide master, see Changing Master in the Nationwide System on page 137.

7.6.1
Connecting Slave AuC to Another Master

Procedure:

1. From the AuC client main window, select the **Nationwide** tab.

   The **Nationwide** tabbed pane appears.

2. From the main AuC Client menu select **Nationwide** → **Change Master...**

   NOTE: You can change the master only when the connection with current master is inactive. To disconnect with current master select **System>Go Out of Service** from the main AuC Client menu on the Master AuC.

   You are prompted for IP address of new Master AuC.

3. Insert the IP address of new Master AuC and press **OK**.

   The Master AuC and the Slave AuC are listed in the **AuC Net**. Initially the status of the Master AuC is **Connecting...**

4. Wait until the Slave AuC connects to the Master AuC. The slave will be able to connect to the Master AuC only when its IP address is set in the Master AuC as the IP address of the Expected Slave AuC. To learn how to add Expected Slave, see Adding a New Slave AuC to the Nationwide System on page 135. To learn how to change Expected Slave, seeChanging Expected Slave AuC on page 135 .

   The Slave AuC tries to establish the connection with the master every 5 minutes until it succeeds. When the Slave AuC connects to the master the status of the master listed in the **AuC Net** window changes to **Connected**.

7.6.2
Changing Master in the Nationwide System

Procedure:

1. On the Master AuC, from the main menu select **Nationwide** → **Transform to Slave**

   The local AuC is listed in **AuC Net** as a slave and there is an **Unknown** server is place of master AuC.

2. On the Slave AuC that is to become Master AuC from the AuC client main window, select the **Nationwide** tab.

   The Nationwide tabbed pane appears.

3. From the main AuC Client menu select **Nationwide** → **Transform to Master**.

   NOTE: This option is only available when the current connection with Master AuC is inactive.

   The Slave AuC transforms to master. It keeps information about the previous network configuration, therefore you dont need to provide IP addresses of other Slave AuCs.

4. On the remaining Slave AuCs replace the existing Master AuC with the new one. For information how to change the master, see Connecting Slave AuC to Another Master on page 137.

   The Slave AuCs connects to the new Master AuC. You can monitor this process in the **AuC Net** window on Master AuC.

5. On the previous Master AuC Server from the main menu select **Nationwide** → **Change Master**.

   You are prompted for the IP address of the new Master AuC.

6. Insert the IP address of the new Master AuC and press **OK**.

   NOTE: On Master AuC check on the **Nationwide** tab whether all Slave AuCs are connected to the nationwide AuC system. For more information on how to view the status of each AuC in the nationwide AuC system, see Viewing AuC Connection Information and Status on page 128.

   The AuC Server is connected to the Master AuC.

Chapter 8

AuC System Settings

8.1 Configuring Authentication Centre Operation Settings

8.1.1 Configuring KVL Port Settings

Configure the KVL port settings in the AuC/PrC Client application to enable the AuC/PrC to KVL direct communication or serial modem communication.

Procedure:

1. From the **System** menu, select **Preferences**.
2. In the **Preferences** window, in the tree view on the left, select **Port Settings**.
3. Perform one of the following actions:

If...	Then...
You want to enable the AuC/PrC to KVL direct communication,	perform the following actions: a. Under **Port settings for Key Variable Loader connection**, configure the following settings: i. **Port:** • For AuC, use **COM1**. • For PrC, use **COM2**. ii. **Type:** • For AuC, select **AuC**. • For PrC, select **PrC**. iii. **Connection:** Select **Direct**. iv. **Bit Rate:** Leave the default value (**19,200**). Ensure that this value matches the value set on the KVL. b. Click **OK**.

If...	Then...
You want to enable the AuC/PrC to KVL serial modem communication,	perform the following actions: **a.** Under **Port settings for Key Variable Loader connection**, configure the following settings: **i.** **Port:** • For AuC, use **COM1**. • For PrC, use **COM2**. **ii.** **Type:** • For AuC, select **AuC**. • For PrC, select **PrC**. **iii.** **Connection:** Select **Modem**. **iv.** **Bit Rate:** Select **19,200**. **b.** Ensure that `ATM0S0=1` appears in the **Initialisation String** column. **c.** Click **OK**.

The settings are saved.

IMPORTANT: On the server rear panel, the COM1 port is labeled **AuC** and the COM2 port is labeled **PrC**. Use these ports accordingly when establishing the connection.

8.1.2
Configuring Miscellaneous Settings

Procedure:

1. Select **Preferences** from the **System** menu.

   The **Preferences** window appears. Miscellaneous entity is already highlighted.

2. Make sure the **Stop box synchronization during nationwide CMG operation** checkbox is checked in order to prevent box synchronization during nationwide CMG operations. This option is enabled by default.

   IMPORTANT: Disabling the **Stop box synchronization during nationwide CMG operation** checkbox can lead to inconsistency of key material in boxes across different clusters. It should only be used if an urgent need to synchronize boxes with AuC, despite ongoing nationwide CMG changes, exists.

8.1.3
Configuring Server Settings

Procedure:

1. Select **Preferences** from the **System** menu, then select **Server Settings** entity in the tree view on the left.
2. Enter the **Server ID** (for communicating with KVLs) and **Server Alias** (How the AuC appears in nationwide listings). You can also check the **Debug Log Enabled** if you want the debug log to be maintained on the server.

8.1.4
Configuring User Settings

The User Settings allows a User Administer to change the security level for all future user names and passwords. The User Settings consist of length constraints, consistency, and change interval requirements. The AuC comes with default settings. These default settings can be changed, but the changes will only be applied when users attempt to change their password.

IMPORTANT: It is highly recommended to maintain user settings complexity to ensure a secure system.

Procedure:

1. From the **System** menu, select **Preferences**.
2. In the **Preferences** window, select the **User Settings** entity in the tree view on the left.
3. Adjust all the restrictions you want applied to passwords and click **OK**.

   NOTE: If changing the user settings makes current passwords non-compliant, the affected users are asked to change their passwords next time they log on.

   The new settings are stored in the AuC database.

8.1.5
Configuring SAI Cache Settings

Procedure:

1. Select **Preferences** from the **System** menu.
2. Select the **SAI Cache** entity in the tree view on the left.
3. If the **Auto Cache Population** option is selected every 15 minutes SAI keys are being generated for mobiles which do not have SAI keys in their cache. Maximum 1000 keys can be generated at one time. You can clear the **Auto Cache Population** option and generate or clear the SAI keys using **Fill** and **Clear** buttons.

8.1.6
Configuring Thresholds Settings

The **Thresholds** dialog box allows configuring thresholds monitoring. To change the thresholds monitoring state, follow the procedure below:

Procedure:

1. From the **System** menu, select **Preferences**.

   The **Preferences** dialog box appears.

2. Select **Thresholds** entity in the tree view on the left.

   The **Thresholds** dialog box is displayed in the right pane of the **Preferences** dialog box.

3. **GSKO OTAR threshold** configures the percent of mobiles required to confirm. Enter a new number in the text entry field or use the up and down arrows.
   - inactive GSKO prior to GSKO activation
   - active GSKO prior to OTAR AIE key activation.

4. **GCK OTAR threshold** is the percent of mobiles required to confirm inactive OTAR AIE key prior to GCK key configuration. Enter a new number in the text entry field or use the up and down arrows.
5. **TM SCK OTAR threshold** is the percent of mobiles required to confirm inactive OTAR AIE key prior to TM SCK key activation. Enter a new number in the text entry field or use the up and down arrows.
6. **DM SCK OTAR threshold** is the percent of mobiles required to confirm inactive OTAR AIE key prior to DM SCK key activation. Enter a new number in the text entry field or use the up and down arrows.
7. **CCK update threshold** is the percent of sites with current AIE key required to start and proceed with CCK key update. Enter a new number in the text entry field or use the up and down arrows.
8. **GCK update threshold** is the percent of sites with current AIE key required to start and proceed with GCK key update. Enter a new number in the text entry field or use the up and down arrows.
9. **DM SCK update threshold** is the percent of sites with current AIE key required to start and proceed with DM SCK key update. Enter a new number in the text entry field or use the up and down arrows.

Chapter 9

Encryption Device Configuration

9.1 Viewing Encryption Device Status

The Authentication Centre (AuC) utilizes an encryption device to perform encryption services.

Procedure:

1. From the **System** menu, select **Encryption Device**.

   The **Encryption Device** dialog box indicating the status of the encryption device appears.

2. The **Master Key Status** has influence on the encryption device status. For example, if **Master Key Status** is not **Loaded** device status is **Failed**. The **Supported Algorithms** have influence on the encryption device status. For example, if not all algorithms are supported device status is **Failed**.

9.2 Encryption Device Information

The **Encryption Device** window provides the following information:

Field	Value
DVI-XL Master Key Status	Loaded
	Not loaded
	Invalid
	Unknown
AES Master Key Status	Loaded
	Not entered on the server
	Invalid
	Not Available
Device Status	Working
	Failed **NOTE:** If the status of the User or Admin password is different than OK, the device status is Failed.
User password status	OK
	CryptR password is invalid
	CryptR password not entered
	CryptR password has been reset
	CryptR password change required
Admin password status	OK

Field	Value
	CryptR password is invalid
	CryptR password not entered
	CryptR password has been reset
	CryptR password change required
Battery Level	Full
	Dead
	Unknown
Supported Algorithms	List of required algorithms. When the algorithm is installed on the encryption device, the corresponding check box is selected: • DVI-XL • AES-128 • Hurdle-II 128 Bit • Hurdle-II 80 Bit

9.3 CryptR2 Configuration for Standby AuC

CryptR2 configuration can be performed only on active AuC. If you want to configure CryptR2 on standby AuC perform the following actions.

Procedure:

1. Log on to the new standby AuC server (auc02) using Remote Desktop.
2. Start Config Assistant by right-clicking the desktop shortcut. Select **Run as administrator**.

   You need to be an Administrators group member.
3. Activate application only by executing command: `ca role active --application`
4. Perform any desired procedure from Configuring CryptR2 on page 146.

   NOTE: Use standby AuC IP address or host name when starting AuC client.
5. Switch back application to standby role by executing command: `ca role standby`

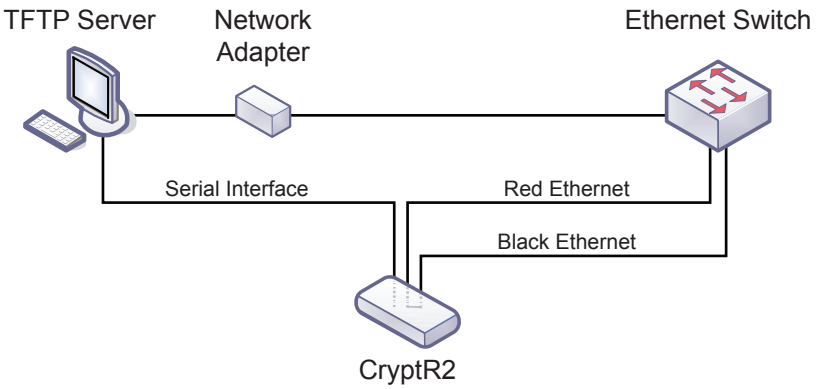
9.4 Upgrading the CryptR2 Software Through TFTP

NOTE: TFTP upgrade erases all keys from the CryptR2.

Procedure:

1. Connect CryptR2 to the TFTP server through an Ethernet switch and Ethernet cables (as shown below).

Figure 47: CryptR2 Connection Diagram



NOTE: If the TFTP server is installed on the PC that runs on a terminal, and not a standalone PC, you also need to install a network adapter (such as an Ethernet PC card or a USB Ethernet adapter) on your PC.

2. Configure the TFTP server and Ethernet switch with the following information:
   - Ethernet switch IP address: 192.168.0.1 (see the *System LAN Switches* manual).
   - TFTP server PC IP address: 192.168.0.187
   - TFTP server PC mask: 255.255.0.0
   - TFTP server PC gateway: 192.168.0.1
3. If a firewall is blocking data transfer, contact your administrator to temporarily disable or remove the firewall.
4. Start the TFTP server if it cannot run as a background task. For example, double-click the **Tftp32** icon on the desktop, if the TFTP Server is Tftp32.
5. Transfer the `red_cryptr_upgrade.bin` and `blk_cryptr_upgrade.bin` binary images to the TFTP server. Store the image files in `c:\Programming Files\Tftp32` (if the TFTP server is Tftp32).

   NOTE: The name of the images file must be `red_cryptr_upgrade.bin` and `blk_cryptr_upgrade.bin`
6. Initiate a connection with CryptR2 and log on.

   NOTE: You need to log on as `admin` to be able to perform the upgrade.

   The prompt appears:

   ```
   CRYPTR>
   ```
7. Enter the following command to program the Red PIKE: `progconf all`

   After a successful upgrade of the RED PIKE, the Power LED is set to green.
8. Press the Erase button on the CryptR2 to program the Black PIKE.

   After a successful upgrade of the Black PIKE, the Power LED is set to green. If the Power LED is not set to green, or if the Tx Clear LED is set to orange, it means that the upgrade failed. In this case, see TFTP Upgrade Failure – Troubleshooting on page 146.
9. Reset CryptR2. (Unplug CryptR2, wait few seconds, plug it in and wait till the LEDs stabilize.)
10. Change the Ethernet switch IP address back to the one you replaced in step 2.

9.4.1
TFTP Upgrade Failure – Troubleshooting

Perform the following steps to troubleshoot a TFTP upgrade failure. If the problem persists, contact the Motorola System Support Center (SSC).

Process:

1. Check network connections.
2. Check the USB cable and Ethernet cable condition. Ensure that the Ethernet cable is a straight cable.
3. Check the TFTP server configuration.
4. Check the Ethernet switch configuration.
5. Check the image files name convention.
6. Ensure that the TFTP server is started and running.
7. Ensure that the firewall is disabled.
8. Ensure that image files are stored in the TFTP server under `c:\Programming Files\Tftp32` (if the TFTP server is Tftp32).
9. Use a network monitor tool to monitor the network transfer messages.

9.5
Configuring CryptR2

Process:

1. Set up CryptR2. Follow Setting Up CryptR2 on page 146.
2. Enter users password and then enter admins password for the CryptR2 device and store it on the AuC server. Follow Entering User and Admin Password on page 147
3. Enter AES Master Key on the AuC server (the same password must be entered into the CryptR2 device). Follow Entering AES Master Key on page 148
4. Validate passwords by pressing **Validate** button.

   NOTE: If Device Status appears as Failed – Master Key not loaded, User Password Status and Admin Password Status appears as OK, then the CryptR2 was successfully connected with AuC/PrC and validated both passwords.

   IMPORTANT: After 10 unsuccessful attempts default factory passwords will be restored on the CryptR2 device.
5. Load master keys into an Encryption Device. Follow Loading Master Keys into an Encryption Device on page 148

9.6
Setting Up CryptR2

Procedure:

1. Login to CryptR2, with serial shell using for example PuTTY, as admin.

   You are prompted to change the password.
2. Type in the old password.
3. Type in the new password.

4. Confirm the new password.
5. Type `cryptrconfig`

   You are prompted to set up IPs.
6. Set up IPs as follows:

   Enter RED (trusted network) IP address[192.168.0.204]>10.0.252.11
   Enter RED subnet mask[255.255.255.0]>255.255.255.0
   Enter RED default gateway[none]>
   Enter Host IP address[192.168.1.1]>10.0.252.2
   Enter Host Port Number[Range:49166-65535][49166]>
   You are informed that the parameters were changed
7. Type `exit` to logout.
8. Login to CryptR2, with serial shell using for example PuTTY, as user.

   You are prompted to change the password.
9. Change password as prompted.
10. Type exit and close serial shell.
11. Disconnect CryptR2 from the power source and connect it again.

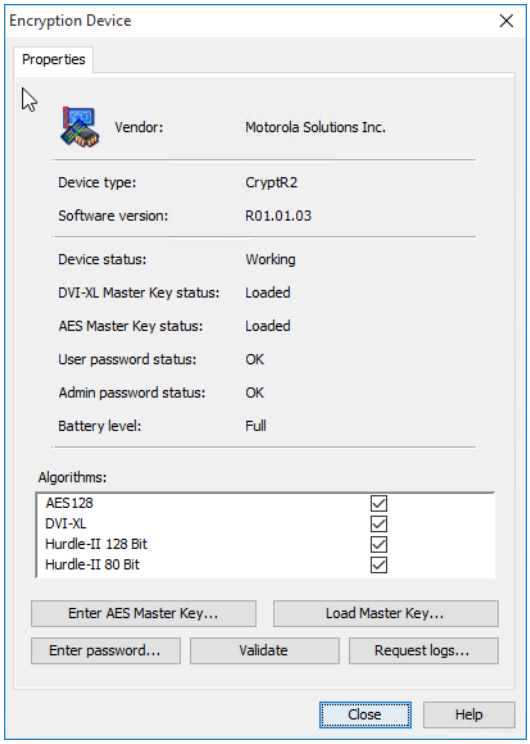
9.7 Entering User and Admin Password

Procedure:

1. Select **Encryption Device** from the **System** menu.

   The **Encryption Device** window appears indicating the status of the encryption device.

Figure 48: Encryption Device Dialog Box



2. Click the **Enter password** button.
3. Select accounts for which you want to enter the password (user, admin) then enter and re-enter password and click **OK**.

9.8 Entering AES Master Key

Procedure:

1. Select **Encryption Device** from the **System** menu.
2. In the **Encryption Device** window, click the **Enter AES Master Key** button.
3. Enter and then confirm Master Key and click **OK**.

9.9 Loading Master Keys into an Encryption Device

The Authentication Centre (AuC) utilizes an encryption device to perform encryption services. To operate, the encryption device requires the loading of a master key.

The encryption device uses the master key to encrypt data stored in the AuC database. The loading of master key into an encryption device must be initiated and performed from the AuC.

Alternatively, you can load the Master Keys using a serial connection. See Loading Keys with Serial Connection on page 150.

NOTE:
If necessary, the existing master key can be reloaded or replaced with a new master key.

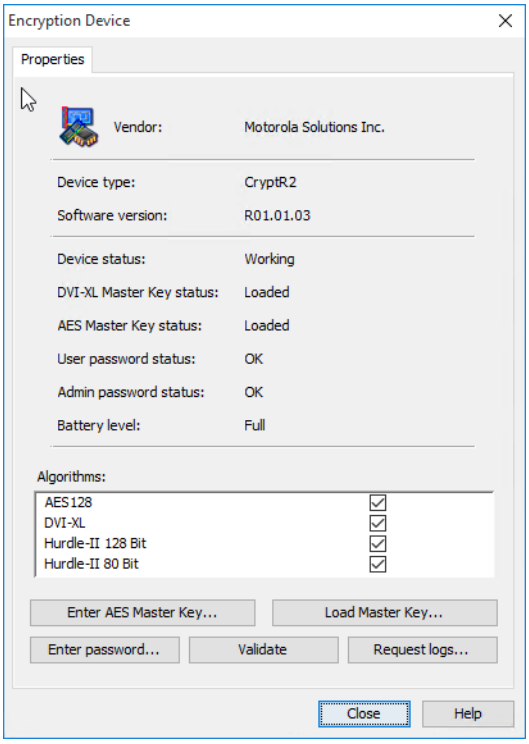
If loading Master Keys for the first time, it is important to load the DVI-XL key first, and then the AES 128 key. If you start loading master keys with AES with no DVI-XL loaded, CryptR2 reports successful load, however AuC reports that operation failed (it is unable to validate AES, because DVI-XL is not loaded).

Procedure:

1. Select **Encryption Device** from the **System** menu.

   The following dialog box is an exemplary output.

   Figure 49: Encryption Device Dialog Box



2. The **Enhanced Authentication Centre Client** displays the encryption device with a status of `Not Loaded`.
3. In the **Encryption Device** window, click **Enter Password** button, then enter passwords for admin and user accounts.
4. Click **Validate** button, in order to validate the passwords.
5. Click **Enter AES Master Key** button, then enter and confirm the key and click **OK**.
6. Click the **Load Master Key** button.
7. In the **Load Master Key for CryptR2** window, select the **DVI-XL** Master Key and the interface you want to use in order to load the Master key, then press **Next**.

   NOTE: You can choose KVL or Serial interface for loading both Master Key types. To load the Master Key using the serial interface, see Loading Keys with Serial Connection on page 150.
8. Click **Next**.

9. Set up the Key Variable Loader (KVL) to load the master key into the encryption device and click **Next**.
10. Click **Next**. You now have 1 minute to load Master Key. Once the process is complete, information that the key load operation was successful appears.
11. Click **Finish**.

    The dialog box window closes.
12. Select **Encryption Device** from the **System** menu.

    NOTE: Device status appears as Failed until you enter the DVI-XL Master Key and AES Master Key.

    .
13. Click the **Load Master Key** button.
14. Select the **AES 128** Master Key and the interface type. Click **Next**.
15. Once the informational messages have been clicked through, the Enhanced Authentication Centre Client allows one (1) minute to use the KVL to load the master key.
16. Select **Crypto Device** option on the KVL from the main menu.
17. From the list of available Master Keys, select **AES 128** key to be loaded into the Crypto Device. Both the KVL and the **Enhanced Authentication Centre Client** displays a confirmation that the master key load was successful.
18. Once the informational messages have been clicked through, and the master key was loaded, the **Enhanced Authentication Centre Client** displays a confirmation that the operation was successful.
19. In the **Enhanced Authentication Centre Client**, select **System** → **Go Operational**.

9.10 Loading Keys with Serial Connection

Procedure:

1. Open the **Enhanced Authentication Centre Client**. From the **System** drop-down menu, select **Encryption Devices**.
2. The **Enhanced Authentication Centre Client** displays the encryption device with a status of **Not Loaded**.
3. In the **Encryption Device** window, click **Enter Password** button, then enter passwords for admin and user accounts.
4. Click **Validate** button, to validate the passwords.
5. Click **Enter AES Master Key** button, then enter and confirm the key and click **OK**.
6. Click **Load Master Key** button, then select DVI-XL key and serial interface.
   a. Once the informational messages have been clicked through, the **Enhanced Authentication Centre Client** allows one minute to use the serial connection to load the master key.
   b. Using the USB to Mini USB cable connect the service laptop to the CryptR2.
   c. Establish a serial connection between the service laptop and CryptR2 using Com*<X>* port, where *<x>* is the serial port assigned to CryptR2. Use the following settings:
      - Baud rate: **9600**
      - Parity: **none**
      - Data bits: **8**

- Stop bits: **1**

d. Log on as **user**

The `mkload>` prompt appears. You are prompted to enter the first master key.

e. Enter the first master key consisting of 128 hexadecimal digits.

You are prompted to enter the second master key.

f. Enter the second master key consisting of 16 hexadecimal digits.

A message confirming that the operation was successful appears.

g. Press ENTER.

h. Return to the **Enhanced Authentication Centre Client**.

Once the master key is loaded, the **Enhanced Authentication Centre Client** displays a confirmation that the operation was successful.

i. Click **OK**.

7. In the **Encryption Device** window, click **Load Master Key** button, then select AES key and serial interface.

a. Once the informational messages have been clicked through, the **Enhanced Authentication Centre Client** allows one (1) minute to use the serial connection to load the master key.

b. Log on as **user**

The `mkload>` prompt appears. You are prompted to enter the master key.

c. Enter the master key consisting of 32 hexadecimal digits.

A message confirming that the operation was successful appears.

d. Return to the **Enhanced Authentication Centre Client**.

Once the master key is loaded, the **Enhanced Authentication Centre Client** displays a confirmation that the operation was successful.

e. Click **OK**.

WARNING: This must be the same Master Key as stored in the **Enhanced Authentication Centre Client** Database. If you change the Master Key, all provisioning related to the Air Interface Encryption infrastructure and radios requires re-provisioning from scratch. For more information, see the *Authentication Centre (AuC) User Manual* manual.

8. Return to the **Enhanced Authentication Centre Client** and perform the following actions:

a. From the main menu, select **System**.

b. Select **Go Operational**.

9.11
Verifying DVI-XL Master Keys

You can verify if the current DVI-XL Master Key loaded into the Authentication Centre (AuC) application matches the Master Key loaded to an encryption device by using the `recrypt` command in the Config Assistant application.

IMPORTANT:
The CryptR device does not support the recryption process with a different System Key (as compared to the one originally loaded with KVL). Therefore, the `recrypt` command from the Config Assistant application will not work in such a scenario.

Ensure that your KVL did not have the System Key changed after loading the Master Key to the AuC. Otherwise, the AuC will transition into the `Encryption Device Failure` state. To change this state back to normal, you have to load the correct Master Key into the AuC by using a KVL with the original System Key. If you do not know the Master Key and do not have the KVL with which you loaded the Master Key into the AuC, you will have to reprovision the entire system.

Prerequisites:

- Ensure that an encryption device with current Master Key is connected to the AuC Server.
- Obtain physical access to the Key Variable Loader (KVL) and the encryption device(s).
- Obtain AuC administrative credentials with Encryption Device Management permissions.

Procedure:

1. Log on to the Authentication Centre (AuC) Server as a user with Encryption Device Management permissions.
2. On the AuC Server desktop, right-click the **Config Assistant** icon and select **Run as administrator**.

   You need to be a member of an Administrators group.
3. In the **Config Assistant** window, enter: `ca recrypt -v`
4. When prompted, provide administrative credentials for the AuC Client application.
5. Connect the KVL to the AuC Server and the encryption device.
6. On the KVL, select the Master Key to verify.
7. Wait for the verification to complete.

Postrequisites: If the Master Keys do not match, perform the following actions:

- Recrypt the AuC/PrC database with a new Master Key (not required on standby AuC). See Changing DVI-XL Master Keys on page 153.
- Update the Master Key on the encryption device(s). See Loading Master Keys into an Encryption Device on page 148 or Loading Keys with Serial Connection on page 150.

9.12

Changing DVI-XL Master Keys

If required, you can replace a Master Key in the Authentication Centre (AuC) Server application by using the `recrypt` command in the Config Assistant application.

Master Keys are automatically propagated to the standby AuC servers, but you need to reload them manually to encryption devices.

IMPORTANT:
The CryptR device does not support the recryption process with a different System Key (as compared to the one originally loaded with KVL). Therefore, the `recrypt` command from the Config Assistant application will not work in such a scenario.

Ensure that your KVL did not have the System Key changed after loading the Master Key to the AuC. Otherwise, the AuC will transition into the `Encryption Device Failure` state. To change this state back to normal, you have to load the correct Master Key into the AuC by using a KVL with the original System Key. If you do not know the Master Key and do not have the KVL with which you loaded the Master Key into the AuC, you will have to reprovision the entire system.

Prerequisites:

IMPORTANT: Authentication and/or provisioning services will be inaccessible for the duration of the reencryption procedure. Verify the impact on service availability before proceeding.

- Ensure that an encryption device with current Master Key is connected to the AuC Server.
- Obtain physical access to a Key Variable Loader (KVL) and the encryption device(s).
- For authentication purposes, prepare the old Master Key or obtain AuC administrative credentials with Encryption Device Management permissions.

Procedure:

1. Log on to the Authentication Centre (AuC) Server as a user with Encryption Device Management permissions.
2. On the AuC Server desktop, as an Administrators group member, right-click the **Config Assistant** icon and select **Run as administrator**.
3. In the **Config Assistant** window, enter: `ca disable`
4. Enter: `ca enable -d`
5. Enter the `recrypt` command with the appropriate authentication option:

If...	Then...
If you want to authenticate through the current Master Key,	perform the following actions: **a.** Enter: `ca recrypt -mk` **b.** Connect the KVL to the AuC Server and the encryption device. **c.** On the KVL, load the old Master Key for authentication.
If you want to authenticate through AuC administrator credentials,	perform the following actions: **a.** Enter: `ca recrypt -c` **b.** When prompted, provide you AuC Client administrator user name and password. **c.** Connect the KVL to the AuC Server and the encryption device.

6. Recrypt the AuC/PrC database with a new Master Key. When prompted, load the new Master Key on the KVL.
7. When reencryption is complete, in the **Config Assistant** window, enter: `ca enable`
8. Log back to the AuC Server with administrative privileges.
9. Ensure that AuC Client is in the `Operational` state. See Changing Authentication Centre Operating State on page 79.
10. Update the Master Key on the encryption devices. See Loading Master Keys into an Encryption Device on page 148 or Loading Keys with Serial Connection on page 150.

9.13 Requesting Logs from an Encryption Device

You can request the logs to verify the condition of the device.

Procedure:

1. From the **System** menu, select **Encryption Device**.
2. In the **Encryption Device** dialog box, select **Request logs**.
3. In the **Save** window, select the location and enter the file name for the log file. Click **Save**.

Chapter 10

System Management

The operation of the Authentication Centre (AuC) requires certain setup and administration tasks to be performed.

10.1 Windows Local Groups

After Authentication Centre (AuC) is installed, new local groups in Windows are created:

- **auc-client-app-local** designed to access AuC Client
- **standby-app-local** designed for Database Standby Manager GUI access

NOTE:
Motorola Solutions recommends creating OS users for each operation. For the application to run, users must be added to groups.

The built-in ServiceUser account is automatically added to the groups during the installation process.

IMPORTANT: Adding a user to a group is not effective until the next logon of that user.

10.2 Config Assistant Access

The Config Assistant application (CA) can be run only by members of an Administrators group by using the **Run as administrator** option.

10.3 AuC Standby Feature

AuC is equipped with redundancy feature as an option. It is realized by standby AuC server installed on separate hardware. This server synchronizes its database with active AuC database in real time. While data replication process is automatic and does not require operator actions (except for installation) – changing role of standby AuC (activation) is manual and requires operator activity.

10.3.1 AuC Roles

AuC server role can be: ACTIVE or STANDBY.

The server role is split in two logical parts:

- Application role – the state of the Database Standby Manager - defining if it is the source (ACTIVE) or the destination (STANDBY) of the data replication, and state of AuC service
- Host role – IP and hostname configuration

10.3.2 Database Standby Manager

The Database Standby Manager is responsible for:

- configuring Database server data replication
- data replication process initialization and error handling
- data replication process monitoring

It is installed as Windows service.

10.3.2.1
GUI Client

The Database Standby Manager GUI client displays detailed status of data replication.

The GUI client is independent of Database Standby Manager service – closing GUI client will not stop Database Standby Manager service.

You can launch the GUI client by double-clicking the **Database Standby Manager** icon placed on the desktop.

At the same time the **Database Standby Manager** icon appears in the notification area showing the status of standby AuC.

Figure 50: Database Standby Manager System Tray Icon

Check Table 91: AuC Server Standby Status Information Icon on page 69 for more information on the status system tray icon.

10.3.2.2
Checking Standby Status

Standby status can be used to indicate connection and synchronization state between active and standby AuC.

Data replication from active to standby AuC starts with base backup file being sent from a active AuC to the standby AuC. Then PostgreSQL Streaming Replication begins. It may happen that some data are not replicated on the standby machine due to for example, network problems.

10.3.3
AuC Roles Management

Configuration Assistant tool is used to check and change AuC server current role.

It is possible to check AuC current role, change role from Active to Standby and vice-versa.

10.3.3.1
Checking AuC Current Role

Procedure:

1. Log on to the AuC server.
2. As an administrator group member, right-click the **Config Assistant** icon on the desktop and select **Run as administrator**.
3. In the **Config Assistant** window, enter `ca role show`

   Step example: Possible roles are:

   - ACTIVE

- STANDBY
- UNKNOWN

NOTE: If application role and host role are NOT equal, the server role is UNKNOWN.

4. Optional: To check the detailed status of AuC server, enter `ca role show –d`

10.3.3.2
Switching Roles of AuC Servers

NOTE:
Even if the server role is UNKNOWN, Config Assistant tries to set the role requested by the user.

Config Assistant does not proceed with changing role if network setup is incorrect (unknown IP address - not following the IP plan).

Procedure:

1. Log onto the Active AuC.
2. As an Administrators group member, right-click the **Config Assistant** icon on the desktop and select **Run as administrator**.

   Config Assistant window opens.
3. Type `ca role standby`.

   You are asked to confirm the operation.
4. Press `y`.

   The following message appears

   ```
   Changing application role to STANDBY...
   ```

   then the Active AuC shuts down.
5. Permanently shut down AuC. See the *Network Management Servers* manuals for detailed instructions on how to shut down application servers.

   NOTE: After the virtual machine shuts down, iGAS automatically tries to restart the application, which can lead to IP conflict.
6. Log onto the Standby AuC.
7. As an Administrators group member, right-click the **Config Assistant** icon on the desktop and select **Run as administrator**.

   Config Assistant window opens.
8. Type `ca role active`.

   You are asked to confirm the operation.
9. Press `y`.

   The following message appears

   ```
   Changing application role to ACTIVE...
   ```

   It can take some time till the action is finished, then the server reboots.
10. Log on to the Core Servers iGAS administration menu and boot the standby AuC. See the *Network Management Servers* manuals for detailed instructions on how to boot application servers.

10.3.3.3

Managing AuC Roles after Failure of Active AuC

IMPORTANT: To avoid possible IP conflicts make sure that active AuC is shutdown before proceeding activation procedure.

In case of failure of the AuC server you need to change the role of the Standby AuC server to became Active. In such a case:

- Verify **Data currency** using Standby Manager GUI Client:

  IMPORTANT: If both values displayed in **Last synchronized** and **Last changes applied** fields are **None** do not proceed with changing roles but reinstall Active_AuC and restore from backup file.

  NOTE: Before proceeding with activation procedure consider data currency of the standby AuC (more recent date from **Last synchronized** and **Last changes applied** fields on Standby GUI Client). If you have newer backup file – reinstall active AuC and restore from that backup file.
- Change the role of the AuC B server (from Standby to Active) like described in Changing the Role of the Standby AuC to Active AuC on page 158.
- Perform required repairs to the damaged AuC A server
- On AuC A install AuC as Standby (choose the Standby option while installing AuC software)

To restore the original state (AuC A = Active, AuC B = Standby) perform Switching Roles of AuC Servers on page 157.

10.3.3.4

Managing AuC Roles after Failure of Standby AuC

In case of failure of the Standby AuC server reinstall the server from iGAS menu selecting standby option while reinstalling. You need to boot standby AuC from iGAS menu after the installation is finished. Database Standby manager is operating.

10.3.3.5

Changing the Role of the Standby AuC to Active AuC

Procedure:

1. Log onto the Standby AuC.
2. As an Administrators group member, right-click the **Config Assistant** icon on the desktop and select **Run as administrator**.

   Config Assistant window opens.
3. Type `ca role active`.

   You are asked to confirm the operation.
4. Press `y`.

   ```
   Changing application role to ACTIVE...
   ```

   The following message appears:
   It can take some time till the action is finished, then the server will be rebooted.

Chapter 11

AuC Maintenance

11.1 Backing up the Database

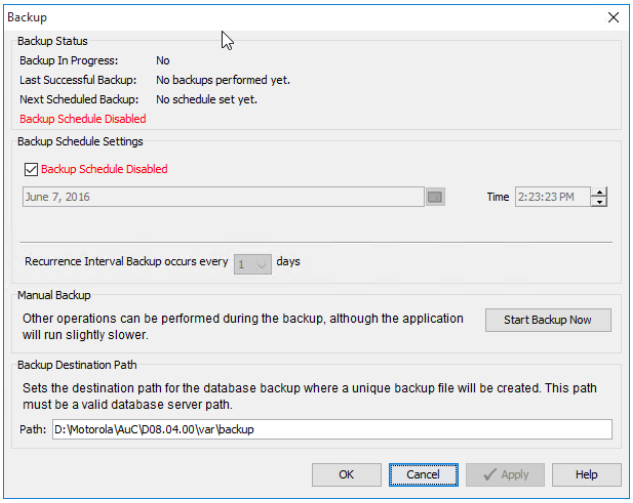
The steps below explain how to backup the AuC database.

Procedure:

1. Select **System** → **Backup** from the AuC client's main menu.

   The **Backup** dialog box appears.

   Figure 51: AuC Backup Dialog Box


Backup
Backup Status
Backup In Progress: No
Last Successful Backup: No backups performed yet.
Next Scheduled Backup: No schedule set yet.
Backup Schedule Disabled
Backup Schedule Settings
Backup Schedule Disabled
June 7, 2016
Time 2:23:23 PM
Recurrence Interval Backup occurs every 1 days
Manual Backup
Other operations can be performed during the backup, although the application will run slightly slower.
Start Backup Now
Backup Destination Path
Sets the destination path for the database backup where a unique backup file will be created. This path must be a valid database server path.
Path: D:\Motorola\AuC\D08.04.00\var\backup
OK
Cancel
Apply
Help

2. Fill in the **Path:** information detailing where you want the backup to be placed.
3. Click **Start Backup Now**.

   The **AuC** dialog box appears.

4. Click **Yes**. The backup of the database starts. The **Backup in Progress** field in the **AuC Database** dialog box changes to **Yes**. The backup icon appears in the **Status Bar** , and there is the `AuC Backup Started` event displayed in the **Events Pane**.

   Figure 52: The Status Bar During Database Backup

5. When the AuC database backup process is completed, the backup icon disappears for the **Status Bar**, and there is the `AuC Backup Complete` event displayed in the **Events Pane**.

Chapter 12

Troubleshooting the AuC

The troubleshooting addresses the most common problems and errors encountered during the setup and operation of the Authentication Centre.

12.1 Basic Troubleshooting

This section covers the following topics:

- Common AuC Start-up Error Messages on page 160
- AuC Troubleshooting Scenarios on page 161
- Scenarios when Performing Key Updates on page 164
- Restarting AuC on page 166
- Key Distribution Failure on page 167

12.1.1 Common AuC Start-up Error Messages

Troubleshooting the Authentication Centre (AuC) client application, you may encounter one or more error messages. These messages are displayed in an alert box. The most common error messages are listed in table below.

Table 98: Common Client Startup Error Messages and Descriptions

Error Message	Description
Server not available. Please ensure the server is running correctly. If the server is rebooting, please wait until it finishes this process.	Displayed when the AuC server machine cannot be located on the network by the client. Make sure that the client has the proper IP address by verifying the DNS configuration. It must be modified if using a different IP address schema than outlined in the IP plan.
This client is incompatible with the server. Please install a server compatible version of the client.	Displayed when the AuC client and server application versions are not compatible.
Root cause of error: Unknown. Please ensure the server is running correctly. If the server is rebooting, please wait until it finishes this process.	Displayed when the AuC server machine is located, but the server application is not running correctly.

There are numerous other error messages that may display during start-up of the AuC client application. These other messages will indicate the root cause and are self-descriptive.

If you are unsuccessful at resolving your client start-up problem, please contact the Motorola Solutions Support for assistance.

12.1.2
AuC Troubleshooting Scenarios

Table 99: Troubleshooting the AuC

Symptom	Possible Cause	Resolution
Getting `Access Denied` message when trying to launch Configuration Assistant.	You are logged in using an account without administrator privileges.	Right-click the CA icon, select **Run as Administrator** and follow the UAC prompts.
AuC becomes stuck in a KEKm update	The AuC has been freshly installed or restored from a very old backup.	Contact the Motorola Solutions Support for assistance.
Radios, zones, KVLs, etc. are not showing up at the AuC when added to the NM Client.	AuC-NM communication problem	Log in to the problem server as admin. Disable the server and then re-enable it. Wait 3 hours. The missing entities should appear in the AuC client after this procedure.
Attempting to download provisioning material and the KVL appears to be successful but nothing is displayed in the KVL list.	• This could be that the entity does not need to be provisioned. • Another cause is that the KVL does not have a zone assigned to it in the NM client.	• Click on the respective entity's **Update Ki** or **Refresh Ki** button and download again. • On the NM Client open the KVL record and assign the proper zone to it.
KVL displays "Cannot load AuC ID. Check connection and KVL ID" when attempting to download provisioning material.	• This means that the KVL ID is not recognized by the AuC and is denied access. • The AuC has not assigned the correct KVL UKEK	• Check the AuC for the KVL ID. If the KVL does not reside in the AuC, add the KVL at the NM Client and it will appear in the AuC client shortly. • Otherwise it could be that the KVL does not have the correct ID assigned to it. This can be changed under the **Settings>KVL ID** Menu.
KVL displays "Unexpected error communicating with device. Please check your connection and try operation again." error when attempting to download provisioning material.	The baud rates on the AuC and KVL do not match.	Serial connection should have the same value for baud rate on AuC and KVL. The baud rate for the specific COM port in Windows OS should also be the same. 1. Check the KVL setting by selecting **Settings → AuC Settings → Baud Rate Menu**. Check the AuC setting for KVL baud rate by selecting

Symptom	Possible Cause	Resolution
		System → **Preferences** → **Port Settings** on the AuC client. If the problem persists, check the baud rate for the specific COM port in Windows OS.
KVL displays "Connected AuC ID value does not match connected AuC ID value." error when attempting to download provisioning material.	The AuC ID and the KVL setting for the AuC ID do not match.	• On the AuC, select the **Preferences** option from the System menu. On the resulting dialog box, click on the **Server Settings** option and note the displayed AuC ID. Then on the KVL go to the **Settings** → **AuC Settings** → **AuC ID** option and edit the AuC ID.
Error message: "Server returned a Remote Exception"	This will occur when the AuC server is having technical problems or when the client has disconnected from the server after initial log in (cable disconnect, server shutdown).	• Log the actions performed before the error occurred, the error message itself, and the time of error. • If the cause of action is not apparent, restart the AuC, and then, as the last resort, the server and the database. • If the problem persists, contact the Motorola Solutions Support.
AuC database backup fails.	Configuration error with database backups.	If the backup files are being copied to a network drive, make sure that the appropriate AUC services have been modified to run as a user that can access the mapped drive. See the *Standalone Authentication Centre (AuC) Server Restoration* or *Clear Standalone Authentication Centre (AuC) Server Restoration* manual for more information about configuring the AuC for backups.
AuC user interface appears to hang.	AuC client, AuC server, or database is having technical problems.	• Wait 5 minutes. For some problems the system will time out and return control back to the client. In other rare cases, the system could just be overloaded, and needs a few more seconds to finish.

Symptom	Possible Cause	Resolution
		• Use the task manager to close down the application and log back in. • Check for connectivity problems. The AuC may have been disconnected from the network. • Use Registry Editor (Regedt32.exe) to view the following key in the registry: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters Confirm that the following registry value exists (add/modify as necessary): Value Name: DisableDHCPMediaSense Data Type: REG_DWORD -Boolean Value Data Range: 0, 1 (False, True) Default: 0 (False) After making changes to the registry, reboot the AuC server.
Connections to infrastructure entities are shown as disconnected on the AuC, but the entity appears to be working correctly.	AuC may have synchronization problems with UCS.	Check the Event Log. If the log has an event which states 'Start synchronizing with UCS' and later there is an event which says 'UCS is disconnected', it means that a synchronization problem occurred. In this case, contact the Motorola Solutions Support for assistance. Otherwise, stop and restart the AuC Client/Server.
No connection with CryptR2 through serial terminal (e.g. Putty)	Serial connection failure.	Disconnect USB cable. Power down and then power up CryptR2.Wait for the red KVL interface LED to blink yellow (2x) or green. When the CryptR2 powers up, you will see the LED initially go yellow, then red and then yellow again. If there is a connection successfully setup, it will turn green. Connect the USB cable. You can use serial terminal now.

Symptom	Possible Cause	Resolution
No connection between the AuC and CryptR2. Encryption device is in “Cryptr is down” state.	Ethernet cable is not connected or IP addresses are not configured correctly.	Check cable connections and IP settings.
Encryption device is in “Battery is dead” state.	Battery is dead.	Replace battery in CryptR2.
Encryption device is in “Invalid password” state.	Passwords on AuC and CryptR2 do not match.	Align passwords on AuC and on Cryptr2, then perform “Validate” action.
Encryption device is in “Tampered ” state.	Mechanical damage.	Click “Request Logs” button in the Encryption Device window on the PrC. If it does not help, logon with serial interface as admin, perform “errorlog retrieve” command and power-down and then power-up CryptR2.
Encryption device is in “Failed” state.	Invalid or missing master key.	Load correct master key to CryptR2. Make sure AES is entered on AuC.

NOTE: In general, if the user is concerned that the AuC client is showing invalid or incorrect data, the user should restart the client.

12.1.3
Scenarios when Performing Key Updates

There are a number of general scenarios that can happen when performing nationwide and non-nationwide key updates. The nationwide key types are System KEK (KEKm).

12.1.3.1
Scenario 1 Key Update Stuck (Local Cluster)

In this scenario, local cluster (or single cluster) is waiting for responses from one or more infrastructure devices.

Table 100: Scenario 1

Possible Cause	Resolution
• One or more Zones disconnected • One or more Zones not responding to AuC messages • One or more Zones have key mismatch	• Click on the **Devices** tab on the AuC. Then highlight each infrastructure entity relevant to the respective update and determine which entity or entities are not updated for the key update taking place. For each entity that is not updated perform an audit trail search based upon that entity type and its ID. Check for negative acknowledgments (NACKs). The AuC will automatically respond to NACKs with keys synchronization. If synchronization fails, device will be marked as Blocked (red). If no NACKs are visible in the audit trail, the Zone Controller has not responded yet. Either dis-

Possible Cause	Resolution
	able and re-enable the entity for key updates or wait an hour (timeout). If NACK was received with reject reason Decryption Failure for KEKm update, entity will need to refresh Ki.For Ki refreshing, see the steps on provisioning Ki.If NACK was received with another reject reason try to use **Resend** button, to force full key synchronization to entity. If that does not help, disable entity and re-enable it after update finishes. Note that `Resend for Zone` will trigger full Authentication Material refresh for this Zone. If entity failed with `Wrong key status response` in event logs, disable entity and re-enable it after update finishes. Use Resend if necessary. If entity is disconnected, make sure it is compatible with AuC server and has correct Ki keys. If it is suspected to have incorrect Ki, refresh Ki for this entity. • The operator can proceed with the update by opting the problem entity out of the update.

12.1.3.2

Scenario 2 Authentication Material Update Stuck (Local Cluster)

In this scenario, local cluster (or single cluster) is stuck during Authentication Material Update / KEKm refresh.

Table 101: Scenario 2

Possible Cause	Resolution
• In large systems, there might be a large number of radios. If this is the case, the AuC will take a long period of time for this stage of the System KEK update, therefore a degree of patience is necessary. • Mismatch of Home Zone Mapping between AuC and Zone Controller	• Check audit and event logs for Nack: Ms unknown. If it appears, there is mismatch of HZM between AuC and ZC. Trigger AuC-UCS synchronization by pressing **Synchronize** button on **Synchronization** tab. Make sure ZC is synchronized with UCS. If everything is synchronized and problem persist, remove problematic radio record(s) from UCM after noting down its properties. When update finishes, try to add it back.

12.1.3.3

Scenario 3 Nationwide Update Stuck (Nationwide)

In this scenario, local cluster finished update phase but Nationwide update is stuck below 100%.

Table 102: Scenario 3

Possible Cause	Resolution
• One of remote clusters is experiencing Scenario 1 Key Update Stuck (Local	• If one of remote clusters is experiencing Scenario 1 Key Update Stuck (Local Cluster) on page 164 or Sce-

Possible Cause	Resolution
Cluster) on page 164 or Scenario 2 Authentication Material Update Stuck (Local Cluster) on page 165.	nario 2 Authentication Material Update Stuck (Local Cluster) on page 165, resolve the problem on remote cluster
• Nationwide synchronization failed	• Go Out of Service and back to Operational on Master AuC and wait for Slave AuCs to connect. This will restart nationwide key synchronization.

12.1.4
Restarting AuC

If Authentication Centre (AuC) appears as disabled in Unified Event Manager (UEM), a restart is necessary.

Prerequisites:

- Ensure that you are logged on to an account with administrative privileges.
- If you already logged on as ServiceUser, right-click the **CA** icon, select **Run as Administrator** and follow the UAC prompts.

Procedure:

1. As an Administrators group member, on the desktop, right-click the **Config Assistant** icon and select **Run as administrator**.
2. Enter: `ca disable` and wait until AuC services stop.
3. Enter: `ca enable` and wait until AuC services start.
4. Restart the AuC client.

12.1.5
Recovering CryptR2 from Tampered State

When CryptR2 goes into a tampered state, the device stops working. It is possible that the CryptR2 device has been damaged or somebody tried to open it. For the device to start working again, you need to check its physical state, download the error logs and send the logs to Motorola Solutions Support.

Prerequisites: Ensure that you are logged on to an account with administrative privileges.

Procedure:

1. From the **System** menu, select **Encryption Device**.
2. In the **Encryption Device** dialog box, select **Request logs**.
3. In the **Save** window, select the location and enter the name for the log file. Click **Save**.

   NOTE: When CryptR2 reboots and reports normal operation, AuC still reports that CryptR2 is in a tampered state until you reboot AuC services.
4. As an Administrators group member, on the desktop, right-click the **Config Assistant** icon and select **Run as administrator**.
5. Enter: `ca disable` and wait until AuC services stop.
6. Enter: `ca enable` and wait until AuC services start.
7. Restart the AuC client.

12.1.6
Key Distribution Failure

When the AuC sends out Key Updates, it will not complete an update, if it does not receive all the Acknowledgments (ACKs) or Negative Acknowledgments (NACKs) from every entity in its database. This is evident when the AuC client displays Key Updates that are 'stuck' at Stage 1, 2, or 3 with any percentage less than 100%. In that situation the following procedure should be performed to complete update.

12.1.6.1
Normal Operation

After initial set up, a number of issues could arise while performing key updates that require operator intervention.

In the event that not all zone hardware is available upon initial set up and the zone has to be disabled for key updates on the AuC, the zone will have to be brought online after the initial zone are already operating with a set of keys. When this occurs, the zone will have to be provisioned prior to any other key update operation. Once provisioned, the AuC will attempt to update the zone with all the current keys. The progress bar in the key schedules tab of the AuC will not reflect the update operations for this zone. The zone can be monitored in the **Devices** tab and will be represented by a green, circular icon with a yellow key in it when all key types for that zone are current for both present and future keys.

In the event that the zone fails in a key update in the first scenario, the first course of action is to resend all keys to the zone by selecting the zone in the AuC client under the **Devices** tab and selecting **Resend**. This will cause the AuC to resend the keys for that zone only. If the zone fails to respond, the process will be repeated - altogether three times at maximum.

In the event that an update appears to be completed for all infrastructure entities except the entity disabled in the third scenario, contact Motorola Solutions Support through the normal channels for assistance.

12.1.6.2
Follow Up Action

Check all other Key distribution Failure Resolution/Workarounds. Then contact Motorola Solutions Support if distribution still fails.

12.2
Known Issues

This chapter covers the following topics:

- Some Connections Between AuC and KVL Stops Because of AuC Inactivity on page 167
- Database Failure on page 168

IMPORTANT: In the event that the resolutions/workarounds stated below do not work, contact the Motorola Solutions Support through normal channels for assistance.

12.2.1
Some Connections Between AuC and KVL Stops Because of AuC Inactivity

Problem description: When a KVL is connected to the AuC and there is no communication between them for some time, the connection may stop.

12.2.1.1
Resolution/Workaround

Do not keep a KVL connected to the AuC for a long time when no communication occurs.

12.2.2
Database Failure

When the AuC switches to the DB failure state, dialog box with an **OK** buton appears. When you click **OK**, the AuC client will be closed.

12.2.2.1
Resolution/Workaround

Track the AuC state at the status bar. If the status bar shows “Database Failure” state verify that the database version is correct and contact Motorola Solutions Support for further instructions.

12.3
Handling Compromised Units

This chapter describes how the DIMETRA system can handle compromised subscriber units.

If theft or inappropriate use of a radio is discovered it can be temporarily or permanently disabled over the air interface.

The Permanent Disable operation requires authentication and encryption therefore it is available only in some Security Classes, while the Temporary Disable/Enable operation is available in all Security Classes.

- **Security Class 1 (SC1)** – In SC1 only Temporary Disable/Enable can be successfully performed. The Permanent Disable is not available for SC1.

12.3.1
Temporary Disabling/Enabling a Radio

When a subscriber radio is lost or its encryption keys are compromised, it can be temporarily disabled until the problem is resolved.

Temporary disabling is intended to protect a network from attack from a compromised MS. It also provides protection against a faulty MS, for example one which causes interference when it makes calls. It stops the MS from making any call services, but maintains mobility services so that the MS can still register with the network and signal when it changes cell.

As a result of Temporary Disable operation the MS disables its MMI and appear non-functional to the user, so that the user is not aware that mobility services are still active. All incoming and outgoing voice, short data and packet data call services are disabled in both TMO and DMO (Direct Mode).

Enabling restores call services to an MS that has previously been temporary disabled. A simple example might be an MS that was lost, and so was disabled, and now has been found again and is in the hands of an authorized user.

NOTE:
The Temporary Disable/Enable state of a radio may also be controlled by the User Enabled flag in the Radio User Configuration record in the UCS. When this flag is set to NO then:

- All calls initiated by the MS are rejected by the ZC.
- All individual and interconnect calls targeted to the MS will be rejected.
- MS will be able to listen to a group calls and broadcast calls.
- All group attachment requests to the MS's selected group will be rejected.

NOTE: Temporary Disable in the RCM is recommended to be used in conjunction with Disable of a Radio User in the UCS. The Temporary Disable command to the radio will cause it to appear dead to the user. If a temporarily disabled radio is sent, for example, a call setup request it will not respond; the call will clear down due to timeouts as if the radio was out of coverage. It is better that the call request does not get issued by the SwMI at all such that there is no waste of control channel bandwidth involving an MS that is never going to respond. This can be achieved by setting the Radio User Object to disabled for the relevant Radio User.

For more information on temporarily disabling a radio, see the *Radio Control Manager* manual.

12.3.1.1
Opening the Radio Command Window in the RCM

You can interact with the web-based RCM application through Chromium.

Procedure:

1. Double-click the **Chromium** icon.
2. In the address field, enter: `https://atr0X.zoneY:50111`

   where
   <X> is the number of RCM server, and
   <Y> is a zone number
3. In the **RCM Web Client** window, click **Log in**.
4. Enter the user name and password. Click **Log in**.
5. In the RCM web application window, from the **RCM** menu bar, select **Commands**.
6. In the **Commands** dashboard, click **+**.
7. To temporarily disable a radio continue with Temporarily Disabling a Radio from Operating on the System on page 169.

12.3.1.2
Temporarily Disabling a Radio from Operating on the System

You can issue commands only to those radios whose primary talkgroup is in your talkgroup attachment list. The talkgroup attachment list is set up in the User Configuration Manager.

Procedure:

1. From the Commands dashboard, select the **Commands** tab.
2. Click the **+** button on the menu.

3. In the **Radio Commands** dialog box, select the **Temporary Disable** command.
4. In the **Talkgroup** field, enter the ID or alias of the target talkgroup into which you want to regroup the radios.

   NOTE:
   - You can enter either an alias or an ID. An ID must be within the valid ID range for the system. Otherwise, it is considered an alias.
   - You cannot enter duplicate radio entries within a single command.
   - You can select only 100 radios. Each radio represents an individual task in a command.
5. Click the **+** button.

   Radios appear in the **Radios** selected list.
6. In the **Comments** field, describe the purpose of the command or the reason for submitting it.
7. Click **Submit**.

   The command appears in the **Command** dashboard where you can modify it when needed.

12.3.2
Permanently Disabling a Radio

Prerequisites: Permanent disabling is intended to protect a network from attack from a compromised or faulty MS. It should be used when the MS is known to have been compromised, or has been suspected of compromise for a long time.

IMPORTANT: Permanent Disable is a one-way function, there is no equivalent enable.

When an MS is permanently disabled, all key material within the MS is deleted (GCK, GSKO, DMO SCK's, K, DCK, CCK, TMO SCK(s)). This also includes end-to-end key material. The ZC will remove the radio user from its register as if the MS had deregistered and provisioning had been withdrawn.

The Permanent Disable operation should only be invoked when it has been determined that an MS is absolutely unrecoverable. When an MS has been lost or stolen, the first step will always be to temporary disable the MS, followed by a disabling of the user in the Radio User Record of the UCM.

NOTE: Permanent Disable is recommended to be used in conjunction with the deletion of the user's Radio Record in the UCS and the deletion of the K-REF association of the disabled MS in the PrC and the AuC that lies within the cluster where the MS's home zone is located. The system operator shall also ensure that the MS's K-REF association is also removed from the other AuCs in the network in due time, if K-REF pairs are duplicated across the network. Note that if this is not performed, the MS could be assigned a new home zone that lies in a cluster where the K-REF association has not been deleted.

To permanently disable a radio first perform steps from Opening the Radio Command Window in the RCM on page 169 and then perform steps below.

NOTE: The Permanent Disable operation is not available while operating in Security Class 1 or in Security Class 2 without authentication.

Procedure:

1. In the Radio Commands dialog box select the **Permanent Disable** command from the Command drop-down combo box.
2. Type a radio alias or ID in the **Radio** field and click the **right arrow** button to move the entry to the **Radios Selected** list. Use the following guidelines: To remove a radio from the **Radios Selected** list, select the radio and then click the **left arrow** button.

- You can enter either an alias or an ID. An ID must be within the valid ID range for the system. Otherwise, it is considered an alias.
- You cannot enter duplicate radio entries within a single command.
- You can select only 100 radios. Each radio represents an individual task in a command.

3. Type a comment in the **Comment** field. Comments can be used for future reference (for example, to describe the purpose of the command and the reason that it was submitted).
4. Click **Submit**.

   The **Confirmation** dialog box appears.

5. Click **Yes**.

   NOTE: After you click **Submit**, you cannot modify a command. The radios in the **Radios Selected** list are the default selection for a new command. If you do not want a new command to be issued to the same radio, you need to remove it from the list.

   Due to radio system limitations and the impact on call traffic, radio commands are sent to radios at a rate of two per second. In case of sending two or more commands to the same radio, a command is send every two seconds.

   After a command is submitted, it appears in the **Command Monitor** window pane. Subsequent actions on the command are monitored via the **Command Monitor** window pane.

6. Select **Command Monitor** from the **View** menu (if the **Command Monitor** window pane is not currently displayed).

   NOTE: The Permanent Disable command cannot be reverted. After clicking the **Revert** button the command status will become **Invalid** and the reject reason field will state "Cannot revert".

   The **Command Monitor** window pane appears.

7. Examine the **Command Monitor** window pane columns for information about the Permanent Disable command (see the *Radio Control Manager* manual for details). The following columns provide key information:

   NOTE: The **Status** column provides an overview of the state of all of the radio tasks for that command. After a radio command is submitted, it transitions through a number of states before completing. See the *Radio Control Manager* manual for a description of command status states as listed in the **Status** column.

   The **Reason** column shows the reject or failure reasons for failed commands. See the *Radio Control Manager* manual for a description of reject reasons as listed in the **Reason** column.

12.4 FAQ

The following topics address common questions and answers for Authentication Centre (AuC) operators and administrators.

12.4.1 Key Management

This section provides answers to some of the Frequently Asked Questions (FAQs) related to key management using the AuC:

- How are Keys Provisioned in the DIMETRA System? on page 172
- How are Keys Stored in the DIMETRA System? on page 172

- How are Keys Updated in the DIMETRA System? on page 172
- What Do I Do if a Key is not Current? on page 172
- When Should I Perform an Audit Trail Search? on page 173
- Key Update Stages on page 173

12.4.1.1
How are Keys Provisioned in the DIMETRA System?

Keys are distributed to new system entities automatically from the Authentication Centre (AuC). The User Configuration Server (UCS) and Zone Database Server (ZDS) applications notify the AuC when a new entity has been added to the system. Upon notification, the AuC obtains configuration information on the new entity from the UCS or ZDS and then generates and distributes the proper keys to the entity.

12.4.1.2
How are Keys Stored in the DIMETRA System?

Keys are stored in the AuC database encrypted on the master key. The master key is stored in the AuC encryption device and used to encrypt/decrypt all database data. Without knowledge of the specific master key, data cannot be read.

12.4.1.3
How are Keys Updated in the DIMETRA System?

The Authentication Centre (AuC) uses two methods to update encryption keys in the system infrastructure.

- scheduled key updates
- on-demand key updates

Both types of updates are executed from the AuC main client window.

When the key update is launched, the AuC performs an encrypted key transfer over the system infrastructure network.

12.4.1.4
What Do I Do if a Key is not Current?

If an infrastructure key (Ki) is not current (signified by a yellow key status icon), you must ensure that the appropriate key variable loader (KVL) has properly loaded the Ki key into the affected zone or base site entity. After successfully loading the key, the KVL must reconnect and return a loading acknowledgment message to the Authentication Centre (AuC). Until this is performed, the AuC considers the entitys Ki key to not be current.

If a system key encryption key (KEKm) or zone key encryption key (KEKz) is not current (signified by a yellow key status icon), verify that links to the User Configuration Server (UCS) and Zone Database Server (ZDS) are connected. If not, you need to perform proper system troubleshooting procedures to determine the cause (such as consulting the UEM fault management application).

If the links are up and there is an overall update occurring for the affected entity, you do not need to do anything. If the links are up and no key update is occurring, you should query the audit trail for that particular entity to further investigate the errors that have occurred.

12.4.1.5
When Should I Perform an Audit Trail Search?

The Authentication Centre (AuC) maintains an audit trail log of all performed key operations. An audit trail can be created when you want to examine key operations (distribution and updates of keys) that have occurred on the system. An audit trail is also a useful tool for troubleshooting problems with key updates.

12.4.1.6
Key Update Stages

A key update cycles through three stages:

Table 103: Key Update Stages

Stage	Description
Stage 1: Activate Future Key	The AuC sends a message to the entities to activate the Future key stored in the entity from the last update. The entities send back an acknowledgment when this stage is completed.
Stage 2: Refresh Dependent Key Material	The AuC refreshes existing dependent keys sealed with the previous key. This is done by sealing the existing dependent key material with the newly activated key, and sending the re-sealed key material back to the entities. In an example, if the Zone Key Encryption Key (KEKz) is updated, all Static Cipher Keys (SCK-TMOs), sealed with the previous KEKz, must be re-sealed with the new KEKz and sent back to the BTS site entities. The entities send back an acknowledgment when this stage is completed.
Stage 3: Update Future Key	The AuC sends a new Future key to be stored in the entity. This key will be activated during the next key update. The entities send back an acknowledgment when this stage is completed.

During each stage, the Update Progress bar displays the stage number and percentage of completion. The progress bar scrolls across until the stage is completed.

When the stage is completed, the next stage is started automatically. When the last stage (Stage 3) is completed, the text "Complete" appears.

12.4.2
Radios

This section provides answers to some of the Frequently Asked Questions (FAQs) related to administering K-REFs for radios using the AuC:

- What Do I Do if a K-REF Pair is Unmatched? on page 174
- When Should I Delete Unmatched K-REF Pairs? on page 174

12.4.2.1
What Do I Do if a K-REF Pair is Unmatched?

For an MS, an Individual TETRA Subscriber Identity (ITSI)-REF pair is stored in the User Configuration Server (UCS) database and a K-REF pair is stored in the Authentication Centre (AuC) database. The two pairs, both associated with a specific radio, are matched by the AuC via the REF value. If unmatched REF values exist between pairs, the associated unmatched K-REF pair is reported in the AuC client window. The display of an unmatched K-REF pair in the Authentication Centre (AuC) indicates one of the following conditions:

- An ITSI-REF pair for the radio has not yet been entered on the system.
- An erroneous ITSI-REF pair has been entered in the UCS database.
- An erroneous K-REF pair has been entered in the AuC database.

It is recommended that you verify that both the ITSI-REF and K-REF pair entries are correctly entered in the system.

12.4.2.2
When Should I Delete Unmatched K-REF Pairs?

Once you determine the cause of the K-REF pair failure and have determined which (if any) radio is affected, you can delete the unmatched K-REF pair. However, it is completely at your discretion as to when you want to delete the unmatched K-REF pair.

12.4.3
General Problems

This section provides answers to some of the Frequently Asked Questions (FAQs) related to general problems that you as a user may encounter when using the AuC.

12.4.3.1
How to Trigger Full Synchronization with UCS

During the regular operation synchronization with User Configuration Server (UCS) is performed automatically by the system. However, if AuC is not fully synchronized with UCS and the UCS status is connected, the synchronization process can be triggered manually.

Procedure:

1. In the **AuC Client** window, select the **Synchronization** tab.
2. In the **Synchronization** tab, **Servers** pane, select the **UCS** icon.

   The **User Configuration Server** appears.
3. In the **User Configuration Server** pane, click **Synchronize**.
4. Wait while the synchronization process proceeds. You can observe the progress on the **Status Bar** to the left.

   The AuC is fully synchronized with UCS.

12.4.3.2
Triggering Full Synchronization with ZDS

During the regular operation synchronization with Zone Database Server (ZDS) is performed automatically by the system. However, if AuC is not fully synchronized with ZDS and ZDS status is connected, the synchronization process can be triggered manually.

Procedure:

1. In the **AuC Client** window, select the **Synchronization** tab.
2. In the **Synchronization** tab, **Servers** pane, select the appropriate **ZDS** icon.
3. In the **Zone Database Server** pane, click **Synchronize**.
4. Wait while the synchronization process proceeds. You can observe the progress on the **Status Bar** to the left.

   The AuC is fully synchronized with ZDS.

12.4.3.3
What Happens if a Key Update Fails?

A key update fails when a target device (zone or Base Transceiver System (BTS) site entity) fails to get updated by the Authentication Centre (AuC). If an initial key update fails, the AuC marks the device(s) affected by the failure as "not current" (yellow icon) and attempts a retry of the key update operation.

Once you determine which entities are not current from the key status display, you can perform a search of audit trail information to pinpoint the specific failure that has occurred.

12.4.3.4
What Do I Do if the Database Fails?

If an error occurs indicating that the database has failed, contact Motorola for assistance.

12.4.3.5
What Do I Do if an Encryption Device Fails?

For the Authentication Centre (AuC) CryptR2 module, refer to the CryptR2 documentation for recommended troubleshooting and repair steps.

12.4.3.6
What to Do if an Error Message Appears when Starting the Client?

When starting up the Authentication Centre (AuC) client application, you may encounter one or more error messages. The most common error messages are listed in table below.

Table 104: Common Error Messages

Error Message	Description
Host unreachable: connect. Please ensure the server is set up and running correctly	Displayed when the AuC server machine cannot be located on the network by the client.
This client is incompatible with the server. Please install a server-compatible version of the client	Displayed when the AuC client and server application versions are not compatible.

Error Message	Description
Connection refused: connect. Please ensure the server is set up and running correctly.	Displayed when the AuC server machine is located, but the server application is not running.
Unknown. Please ensure the server is running correctly. If the server is rebooting, please wait until it finished this process.	Displayed most commonly when starting the client while the server application is starting up.

There are numerous other error messages that may display during start-up of the AuC client application. These other messages indicate the root cause of the problem and are self-descriptive.

If you are unsuccessful at resolving your client start-up problem, please contact Motorola for assistance.

12.4.4
Implementing and Enabling GCK/OTAR

Process:

1. Enter configuration for CMGs to AuC.
   - Configuration of CMGs can be done either manually or imported from files. Import from file is recommended for anything but the simplest of configurations. Follow Importing Mapping Files on page 122 Import of configuration files or Creating CMGs on page 123, Creating ISSI Ranges on page 124, Creating Operational Groups on page 124, Creating GSSI Ranges on page 125 to input of configuration manually.
   - Activate Each CMG in configuration. Follow Enabling CMGs on page 123 for each CMG within the configuration.
   - Assign GCKNs to GCK aliases. Follow Assigning GCKNs and KAGNs on page 123. It is recommended to use auto-assign function
   - Assign KAGNs to KAG aliases. Follow Assigning GCKNs and KAGNs on page 123. It is recommended to use auto-assign function
2. Enable a Crypto configuration.

   NOTE: Before any OTAR can be enabled the configuration needs to be enabled. If enabling in a nationwide system the CMG configuration will then be propagated to all slave AuCs. (In a nationwide system this may trigger a TMO-SCK update if an SCK-update in nationwide mode has not been carried out previously.)
3. Configure associations to subscribers. To ensure the subscribers associate the correct keys (SCKNs and/or GCKNs) with the correct talkgroups mappings are exported from the AuC and imported to the subscriber. Each subscriber must have the correct mappings for its CMG so export and import must be organized into CMG. For Motorola Subscribers import is carried out from CPS, for other manufacturers terminals refer to terminal instructions.
   - Export GCKN->TM-GSSI mappings by following Exporting CMG Mappings on page 122.

- Export KAGN->DM-GTSI mappings by following Exporting CMG Mappings on page 122.

  NOTE: Repeat export once for each CMG. For example export CMG A mappings for import to subscribers which are in CMG A, export CMG B mappings for import to subscribers which are in CMG B

  NOTE: Repeat export once for each CMG. For example export CMG A mappings for import to subscribers which are in CMG A, export CMG B mappings for import to subscribers which are in CMG B

  IMPORTANT: The AuC exports KAG->GTSI mappings. The AuC will use the System Country and Network Codes to calculate the GTSI. This means if the Mobile Network Codes and Mobile Country Codes configured for your DMO groups is different to the System codes the GTSI will be different and the association will not be made within the subscriber.

- Read in radio codeplug to CPS
- From CPS menu select File->Import GCKN, then browse to input file (GCKN_TO_GTSI.mou) for appropriate CMG
- From CPS menu select File->Import SCKN, then browse to input file (SCKN_TO_GTSI.mou) for appropriate CMG
- Write codeplug back to subscriber to complete operation

4. Enabling GSKO OTAR by following OTAR Configuration on page 127 for each CMG. This will enable the subscriber populations to be provisioned with GSKO and will also provision the subscribers with the CMG GTSI. After enabling GSKO OTAR for a CMG the SwMI will push GSKO to the subscribers in the CMG on the next mobility action. Therefore it is advisable to allow some time for GSKO to propagate across the subscriber population before enabling further OTAR types.
5. Enable GCK OTAR for each CMG by following OTAR Configuration on page 127. Subscribers will pick up future GCKs from these background broadcasts and can also request current keys from the SwMI. Once sufficient subscriber currency of the initial future GCK has been reached then from AuC initiate a GCK Update by following Scheduling Key Updates on page 113 for GCK key type. Once sufficient subscriber currency of the new future GCK has been reached from ZCM enable GCK operation for all sites as described in **Authentication and Encryption Overview** manual.

   NOTE: At this stage sites should not yet have been enabled for SC3G operation. On enabling GCK OTAR for a CMG the AuC(s) will distribute to all sites the TMO-Association table, MGCKs and GCK OTAR material. The sites will also begin to transmit in a background loop GCK OTAR provides to the CMG(s) GSSI.

6. Enable DM-SCK OTAR.

   IMPORTANT: Before DM-SCK OTAR can be enabled the AuC has to be in 2 key TM-SCK mode.

   - Follow Modifying an SCK-TMO Key in the Authentication Centre on page 98 selecting SCKN 30 as the next active. (If an SCK update does not automatically start then manually start an SCK update to activate SCKN 30)
   - Once SCKN30 is the active key and SCKN31 is next active click on select 2 TMO on AuC GUI.
   - On UCM in each cluster enable Secure DMO as described in **Authentication and Encryption Overview** manual.
   - Enable DM-SCK OTAR by following OTAR Configuration on page 127

7. Enabling TM-SCK OTAR

   NOTE: Subscribers will pick up future TM-SCKs from these background broadcasts and can also request current keys from the SwMI. Subscribers can also request TM-SCK as part of the registration procedure in the same way CCK is retrieved on earlier SC3 DIMETRA releases.

   - Enable TM-SCK OTAR by following OTAR Configuration on page 127.

- To select Raw key mode follow Entering a DIMETRA Distribution Key on page 103 or Generating Raw Keys Automatically on page 103.
- On AuC GUI go to TM-SCK table and select Use Raw Key
- Two TM-SCK key updates are required after raw key mode has been selected before the active TM-SCK will be a raw key

NOTE: If the entire encrypted subscriber population supports SCK-OTAR then the AuC may be switched to raw key mode. This means that the TM-SCKs will be generated either by the AuC encryption device or selected randomly from a pool of imported raw keys. TM-SCKs will only be provisioned to the mobile by OTAR and cannot be exported for manual import to subscribers. The entire encrypted subscriber population will have to be a member of a CMG for TM-SCK to be switched to raw mode.

12.4.4.1

Good Practices

If you intend to change the GSSI ranges in the TMO-TABLE (GCKN->Talkgroup ranges, also known as the KAR) then you must:

- Disable all sites for GCK encryption before making changes.
- Export the updated KAR file (GCKN_TO_GTSI.mou) from the AuC and update all CMG radios affected by changes (It may be advisable as a precaution to update radios in all CMGs.
- Re-enable GCK encryption for all sites only when all steps above have been completed.

When enabling GCK OTAR for either single or multiple CMGs:

- Disable all sites for GCK encryption before enabling OTAR for CMG(s):
- Ensure all radio in affected CMGs are current with GCKN->Talkgroup associations.
- Enable all sites for GCK encryption only when AuC has updated all sites and affected subscribers have been updated.

When disabling GCK OTAR for either single or multiple CMGs:

- Disable GCK encryption for all sites before disabling.
- Affected radio (members of CMGs GCK OTAR disabled for) must be updated to remove associations.
- GCK encryption should only be re-enabled for all sites when AuC has updated all sites (sites will be green icon) and radio which are members of affected CMGs have been updated.

If you change the Talkgroup to KAG ranges then you must export the KAG file (SCKN_TO_GTSI.mou) from the AuC and update all CMG subscribers in updated CMGs (It may be advisable as a precaution to update radio in all CMGs).

Radios are provided with GCK associations when affiliating to a GCK mapped Talkgroup when site is operating in GCK mode(SC3G), therefore it is preferable that subscribers only have GCK mapped talkgroups applicable to their CMG in their talkgroup lists.

If a radio has CMG GTSI erased then the subscriber should be disabled then re-enabled for key updates from the home AuC (see Assigning New Authentication Material for a Radio on page 115).

When adding GCK/KAG mapped Talkgroups to a (Motorola) radio via CPS re-import GCK/KAG associations to ensure new talkgroup has correct association.

12.4.5

Security Class 3 Configuration Changes

The system does not support Crypto Management Group (CMG) configuration changes dynamically while on the Security Class 3[G]. This includes GCK group, TM-SCK group changes, CMG changes, etc. Follow the process below to implement the GCK configuration changes once the configuration is changed.

Procedure:

1. Take system (sites) out of SC3G as described in *Authentication and Encryption Overview* manual.
2. Update AuC CMG configuration see Crypto Management Group Configuration on page 122 for more information.
3. Update associations in all affected radios by opening each TG in CPS and resetting the GCK association manually.
4. Move sites back to SC3G as described in *Authentication and Encryption Overview* manual.

Chapter 13

Config Assistant

Configuration Assistant is a console tool, installed together with the AuC application, allowing you to manage the server for example perform database backup/restore operations, configure and control services. You can also change roles of the AuC servers using **Config Assistant**. Switching Roles of AuC Servers on page 157 and Changing the Role of the Standby AuC to Active AuC on page 158 provide more details on this functionality.

The Config Assistant application (CA) can be run only by members of an Administrators group. To start the application, right-click the **Config Assistant** icon and select **Run as administrator**. Config Assistant window appears listing available commands together with their descriptions. It also shows the list of optional arguments available for each command.

Table below lists commands available from **Config Assistant** tool.

Table 105: Config Assistant Commands

Command	Subcommand	Description	Required Parameter
audit		lists status of 10 last database operations (for example backup, restore)	N/A
restore		performs restoration and, if needed, migration of the database	backup file name
backup		performs hot backup (on running system), backup is stored in a compressed file	backup file name
dbreset		deletes entire content and schema from the database and then enters clean schema to the database	N/A
enable		starts all the services	N/A
disable		stops all installed services	N/A
status		shows the status of all services	N/A
detailed_status		shows comprehensive application status	N/A
srvcfg	show	shows services startup type	N/A
	auto	changes services startup type to automatic	N/A
	manual	changes services startup type to manual	N/A
swinfo		shows software version	N/A
logs	clear	deletes old log files	N/A
	collect	collects logs of all components (server, client, db...)	output file name
migrate		migrates data during an update	N/A

Command	Subcommand	Description	Required Parameter
csreport		collects logs from the application for support purposes in one compressed file	output file name
encryption	show	shows current encryption device	N/A
role	show	shows current role	N/A
	active	changes role to active	N/A
	standby	changes role to standby	N/A
keysreport		exports zones/sites keys version report (from the database or backup file)	N/A
csappaccount		resets password for application admin account	N/A
csdbaccount		resets password for database support account **NOTE:** Command allows to change password for support account in the database. It should only by used by Motorola support team.	N/A
exportki		exports Ki keys from the Authentication Centre client to a file **NOTE:** The device number is a numeric label and comprises of the following elements: • single number – for zone controllers • two numbers (e.g. 2:2) – indicate the Base Transceiver Station number and zone	-f *<filepath>* -d *<device number>*
importki		imports Ki keys from a file to the Authentication Centre client	-f *<filepath>* -d *<source device number><target device number>* -cf *<filepath and name of the control file>* (the file with a sequence of instructions for a parameter)
recrypt		recrypts AuC/PrC database with a new Master Key	N/A

Prompting a command with **–h** argument shows help message for this command and lists optional parameters available for this command together with their descriptions.

In order to perform desired command enter: `ca <command>`, or `ca <command> <subcommand>`. For example in order to disable services type `ca disable` and press **Enter**, in order to delete old log files type `ca logs clear` and press **Enter**.

If you want to display help message for desired command type `ca <command> -h` or `ca <command> <subcommand> -h`.

Table below lists all commands together with their optional parameters and descriptions.

Table 106: Optional Arguments for CA Commands

Command		Parameters	Description
audit		-c N, --count N	show last N audits
restore		-r, --restore-only	restores the database without migration of data
		-q, --quiet	prints only error messages
		-c, --check-file	prints information about backup file, does not perform restore operation
		-S, --standby	switches replication mode on/off
		-R, --recovery	allows to recover from failed or interrupted restore
		-B BACKUPDIR, --backupdir BACKUPDIR	performs restore operation from a directory where the backup file is stored
backup		-q, --quiet	prints only error messages
		-f, --force	forces the backup, enables database if needed
		-B BACKUPDIR, --backupdir BACKUPDIR	allows to determine thr directory where the output file will be stored
dbreset		-q, --quiet	prints only error messages
enable		-q, --quiet	prints only error messages
		-f, --force	keeps trying to enable remaining services if one of them fails
		-d, --database	enables the database service only
disable		-q, --quiet	prints only error messages
		-f, --force	keeps trying to disable remaining services if one of them fails
status		-v, --verbose	prints detailed information about each service status
		-n, --numeric	prints numeric representation of service state
srvcfg	show	-n, --numeric	prints numeric representation of service startup type
	auto	-q, --quiet	prints only error messages

Command		Parameters	Description
		-f, --force	keeps trying to modify config of remaining services if one of them fails
	manual	-q, --quiet	prints only error messages
		-f, --force	keeps trying to modify config of remaining services if one of them fails
swinfo		-v, --verbose	prints additional information about database version
logs	clear	-q, --quiet	prints only error messages
	collect	-q, --quiet	prints only error messages
		-A DIR, --archivedir DIR	allows defining the path to the directory where the output file is stored
csreport		-q, --quiet	prints only error messages
		-m, --minimal	excludes database dump from report
encryption	show	N/A	shows current encryption device
role	show	-v, --verbose	prints host application role
		-d, --details	prints detailed information about AuC role
	active	-q, --quiet	prints only error messages
		-f, --force	forces performing action even if in ACTIVE role
		-a, --application	changes application role only (skips ip hostname management)
	standby	-q, --quiet	prints only error messages
		-f, --force	forces performing action even if in STANDBY role
keysreport		-i FILE, --input FILE	allows defining the path to the AuC backup file
		-h, --help	shows help message and exits (available for all above commands)
exportki		-q	The quiet display option – displays errors only
importki			The quiet display option – displays errors only
recrypt		-h, --help	displays help message and exits
		-v, --verify	verifies current Master Key. AuC credentials are used for user authentication
		-c, --credentials	uses authentication by AuC user credentials and permissions
		-mk, --master_key	uses authentication by old Master Key verification (this is the default authentication option)